

Generating Sequences of $\text{PSL}(2, p)$

Benjamin Nachman^a

^a*Cornell University, 310 Malott Hall, Ithaca, NY 14853 USA*

Abstract

Julius Whiston and Jan Saxl [19] showed that the size of an irredundant generating set of the group $G = \text{PSL}(2, p)$ is at most 4 and computed the size $m(G)$ of a maximal set for many primes. We will extend this result to a larger class of primes, with a surprising result that when $p \not\equiv \pm 1 \pmod{10}$, $m(G) = 3$ except for the special case $p = 7$. In addition, we will determine which elements of $\text{PSL}(2, p)$ can be in irredundant generating sets of lengths less than or equal to 4 in most cases. We also give some remarks about the behavior of $\text{PSL}(2, p)$ with respect to the replacement property for groups. In the end we state a conjecture for $m(G)$ for all primes with some results from supporting computations.

Keywords: generating sequences, general position, projective linear group

1. Introduction

The two dimensional projective linear group over a finite field of characteristic p , $\text{PSL}(2, p)$ has been extensively studied since Galois, who constructed them and showed their simplicity for $p > 3$ [20]. One of their nice properties is due to a theorem by E. Dickson, which shows that there are only a small number of possibilities for the isomorphism types of maximal subgroups. From this list, one can break up the maximal subgroups into two types: ones that exist for all p and ones that exist for an exceptional list of primes. A more recent proof of Dickson's Theorem can be found in [15] and a complete proof due to Dickson is in [6].

Theorem 1 (Dickson). *The maximal subgroups of $\text{PSL}(2, p)$ are isomorphic to one of the following groups:*

Email address: `bpn7@cornell.edu` (Benjamin Nachman)

1. G_p
2. D_{p-1} , the Dihedral Group of order $p - 1$
3. D_{p+1}
4. A_4 , S_4 or A_5 ,

where G_p is the Frobenius group of order $p(p - 1)/2$ that has a natural description as the semi-direct product $Z_p \rtimes (Z_p^*)^2$. Moreover, while subgroups of types (1), (2) and (3) always exist, a maximal subgroup isomorphic to S_4 exists if and only if $p \equiv \pm 1 \pmod{8}$, subgroups isomorphic to A_5 exist if and only if $p \equiv \pm 1 \pmod{10}$ and subgroups isomorphic to A_4 are maximal if and only if $p \equiv 3, 13, 27, 37 \pmod{40}$.

The exceptional maximal subgroups are thus A_4 , S_4 and A_5 . Whiston and Saxl [19] have shown that these exceptional groups play a crucial role in describing the size of generating sets. A generating set $\{g_i\}$ or sequence $\{g_i\}_{i \in I}$ for the group G is called *irredundant*¹ if after removing any g_j from the set or sequence, the new collection no longer generates G . We will denote² by $m(G)$ the maximum length of an irredundant generating set of G . In response to Whiston's description of $m(G)$ for S_n [17], Cameron and Cara described the irredundant generating sequences of maximal length [2]. In the same spirit, we will describe which elements can appear in generating sequences of any length up to the maximal length in $\text{PSL}(2, p)$ in most cases. This size has been determined by Whiston and Saxl [19] for all primes such that the exceptional groups S_4 and A_5 are not maximal in $\text{PSL}(2, p)$.

Theorem 2 (Whiston and Saxl). *Let $G = \text{PSL}(2, p)$, p prime. Then, $m(G) = 3$ or 4. If $p \not\equiv \pm 1 \pmod{10}$ or $p \not\equiv \pm 1 \pmod{8}$, then $m(G) = 3$.*

In their paper [19], Whiston and Saxl note that $m(\text{PSL}(2, 7)) = m(\text{PSL}(2, 11)) = 4$. Since then, various computations have been made to show that the maximal length is also four when $p = 19$ and $p = 31$. The conjecture in [14] is that this small list of primes constitutes the entire collection. The strategy presented here does not easily extend to the case of $p \equiv \pm 1 \pmod{10}$, but a large part of this surprising conjecture is proved in this paper, summarized in the following theorem.

¹In other places in the literature, this same property is called *independent*.

²This function has also been denoted $\mu(G)$.

Theorem 3. *Let $G = \text{PSL}(2, p)$, p prime. If $p \not\equiv \pm 1 \pmod{10}$, then, $m(G) = 3$ unless $p = 7$, in which case $m(G) = 4$.*

To begin, we will introduce the idea of the replacement property for groups and how it is related to and useful for constructing irredundant generating sequences.

2. Irredundant Generating Sets and the Replacement Property

Linear algebra often forms a concrete base upon which intuition is built for studying more general objects. Understanding generating sequences of groups is no exception - the idea of an irredundant generating set is an analogy to linearly independent sets of a vector space. In the case of vector spaces, the classification of linearly independent sets is simple - all such sets have the same length. This is not the case for groups. If we denote by $r(G)$ the minimum length of an irredundant generating sequence, then clearly $m(G) \geq r(G)$ and in general this inequality is strict. For example, one can easily show based on elementary linear algebra that $\text{PSL}(2, p)$ can be generated by two elements (it cannot be generated by one since it is not cyclic) and so $r(\text{PSL}(2, p)) = 2$. On the other hand for $p > 2$, $|\text{PSL}(2, p)|$ must be even since its order is $p(p-1)(p+1)/2$ (both $p \pm 1$ are even). Therefore, there exist nontrivial elements of order 2. Let H be the subgroup generated by all the elements of order 2. This subgroup must be normal and since it is nontrivial it must be all of G because $\text{PSL}(2, p)$ is simple. Furthermore, two elements of order 2 generate a dihedral group, which is a proper subgroup (dihedral groups are not simple). Thus, there must exist an irredundant generating sequence of length at least 3 (with elements all of order 2) and so $r(\text{PSL}(2, p)) < m(\text{PSL}(2, p))$ for $p > 2$.

Even though irredundant generating sets are not exactly the same as bases for vector spaces, such sets of maximal length do share important properties. For example [4], for finite groups G and H , $m(G \times H) = m(G) + m(H)$, just as $\dim(V \times W) = \dim(V) + \dim(W)$ for V, W vector spaces. However, $m(G)$ and $\dim(V)$ have fundamental differences. For a vector space, every linearly independent subset has length at most $\dim(V)$. For a group, it is not the case that for $H < G$, $m(H) < m(G)$. For example, for $G = \text{PSL}(2, 17)$, $m(G) = 3$ but G has maximal subgroups isomorphic to S_4 , for which $m = 3$ as well. A group which does have the property that for all subgroups $H < G$,

$m(H) < m(G)$ is called *strongly flat* [19]. Two important examples of strongly flat groups that we will consider are S_4 and A_5 [19]. In fact, all the symmetric groups, for which $m(S_n) = n - 1$, are strongly flat [19].

Another important aspect of vector spaces is the elementary fact that any linearly independent set can replace a segment of a basis. Let V be an n dimensional vector space over the field F and let $\mathcal{B} = \{v_1, \dots, v_n\}$ be a basis. Now, take any set $\mathcal{A} = \{w_1, \dots, w_m\}$ of linearly independent vectors in V . Then, a standard linear algebra result says that up to reordering of the v_i , $\{w_1, \dots, w_m, v_1, v_2, \dots, v_{n-m}\}$ is a basis of V . In Dummit and Foote, Theorem 3, Section 11.1 [7], this is called *A Replacement Theorem* and is related to the classical *The Steinitz Exchange Property*. The idea is to generalize this notion of replacing an element of a basis to arbitrary groups. Instead of looking at bases, the generalization is generating sets. Also, instead of replacing many elements of the generating set, the focus will be on replacing a single element. This leads to the following definition [4]:

Definition 4 (Replacement Property). A group G satisfies the *replacement property* for the generating sequence $s = (g_1, \dots, g_k)$ if for any g in G , g not the identity, there exists an i so that $s' = (g_1, \dots, g_{i-1}, g, g_{i+1}, \dots, g_k)$ generates G .

A group G is said to satisfy the replacement property for n if it satisfies the replacement property for all irredundant sequences of length $n = m(G)$. A variation on an argument of Tarski shows that if the replacement property holds for the integer n , then we must have $n = m(G)$ [4]. Why is the replacement property useful? It turns out that the replacement property provides a handle for studying generating sequences of finite groups. For example, knowing if a group satisfies the replacement property can give information about the generating sequence structure of the direct product of groups [4].

Unlike vector spaces, not all groups satisfy the replacement property. Many common groups do satisfy this property, for example all the symmetric groups [4]. However, it does not hold in general. For example, consider $G = Q_8$, the Quaternion group. If we think of G as the elements $\{\pm 1, \pm i, \pm j \pm k\}$, then it is clear that i, j is a generating sequence of G . However, we cannot replace either of i or j in this sequence with -1 because $i^2 = j^2 = -1$ and so $\{-1, i\}$ is a proper subgroup of G . More generally if the Frattini subgroup of

a group is nontrivial, then the nontrivial non-generating elements will cause G to fail the replacement property. For Q_8 , $\{\pm 1\}$ is the Frattini subgroup and so it fails the replacement property. One could modify the definition of the replacement property to exclude such cases. Either way, there are examples of groups which are Frattini free and still fail the replacement property. For example, when $p \equiv +1 \pmod 8$, $\text{PSL}(2, p)$ is such a group. Before showing this, the definition of replacement property must be reworked slightly. This property has been phrased in terms of generating sequences, but it can be restated in terms of certain sets of maximal subgroups. To begin, the notion of a sequence of subgroups being in *General Position* is defined.

Definition 5 (General Position). (R. K. Dennis) Let $I = \{1, \dots, n\}$. A sequence (H_1, \dots, H_n) of proper subgroups of a finite group G are said to be in *general position* if $\cap_{i \in J} H_i \subsetneq \cap_{i \in K} H_i$ for all $J, K \subset I$ and $K \subsetneq J$.

It is not yet clear how this is related to the replacement property. Before making this connection, the idea of subgroups in general position needs to be related to sequences. Let (M_1, \dots, M_n) be a sequence of maximal subgroups of a finite group G and let (g_1, \dots, g_n) be a sequence of elements of G . These two sequences are said to correspond to each other if $g_i \notin M_i$ for any $i \in \{1, \dots, n\}$ but $g_j \in M_i$ whenever $j \neq i$. With this connection, there is a relationship between maximal subgroups in general position and irredundant generating sequences [4]:

Proposition 6. *If (g_1, \dots, g_n) is an irredundant generating sequence, then it corresponds to a sequence of maximal subgroups (M_1, \dots, M_n) in general position.*

Proof. Let $H_i = \langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n \rangle$. Since (g_1, \dots, g_n) is an irredundant generating sequence, H_i is a proper subgroup of G . Therefore, there exists a maximal subgroup $M_i \leq H_i$. Note that $g_i \notin M_i$, since M_i is also a proper subgroup, but $g_j \in M_i$ for all $j \neq i$ by construction. Therefore, (M_1, \dots, M_n) corresponds to (g_1, \dots, g_n) . Now, one needs to show that the maximal subgroups are in general position. By construction, for $J \subset I = \{1, \dots, n\}$ then $g_j \in \cap_{i \in J} M_i$ if and only if $j \notin J$. Therefore, the subgroups $\cap_{i \in J} M_i$ are all distinct as no two of them intersect $\{g_1, \dots, g_n\}$ in the same way. \square

Now that a relationship exists between irredundant generating sequences and maximal subgroups in general position, one can construct a criteria on

maximal subgroups for establishing the replacement property. Using the same ideas as in the previous proposition, one can prove the following [4]:

Proposition 7. *Suppose $s = (g_1, \dots, g_n)$ is an irredundant generating sequence of a finite group G and $g \in G$ is an element for which s fails the replacement property. Then, there exists a sequence of maximal subgroups of G corresponding to s such that g is in every M_i .*

Proof. If s fails the replacement property for g , then for each i , the sequence $(g_1, \dots, g_{i-1}, g, g_{i+1}, \dots, g_n)$ generates a proper subgroup H_i of G . Pick a maximal subgroup $H_i \leq M_i$. Then, (M_1, \dots, M_n) corresponds to s by definition and furthermore, $g \in \cap M_i$ by construction. \square

An equivalent (contraposition) statement that is more useful in practice is given below [4]:

Corollary 8. *Suppose that $s = (g_1, \dots, g_n)$ is an irredundant generating sequence of the finite group G . If every sequence of maximal subgroups (M_1, \dots, M_n) corresponding to s intersects trivially, then s satisfies the replacement property.*

Now, we will focus on irredundant generating sequences of $\text{PSL}(2, p)$ which will eventually lead us to study how this group behaves with respect to the replacement property.

3. Irredundant Sequences of Maximal Length in $\text{PSL}(2, p)$

The general strategy for proving that $m(\text{PSL}(2, p)) = 3$ for most cases is to take irredundant generating sequences and try to ‘glue them together’ and see what possibilities exist for the resulting group. We will make this procedure more quantitative as the discussion progresses. In this process, we will switch back and forth between considering elements and (maximal) subgroups corresponding to the elements. Let $g_1, g_2, g_3, g_4 \in G = \text{PSL}(2, p)$ be an irredundant generating set. Let H_1, H_2, H_3, H_4 be the corresponding family of subgroups in general position, i.e. $H_1 = \langle g_2, g_3, g_4 \rangle, H_2 = \langle g_1, g_3, g_4 \rangle$, etc. and let M_1, M_2, M_3, M_4 be a corresponding set of maximal subgroups in general position, i.e. $H_i \leq M_i$, $i=1,2,3,4$. Let $p \equiv \pm 1 \pmod{10}$ or $p \equiv \pm 1 \pmod{8}$. In the course of their proof, Whiston and Saxl [19] show that in the case $m(G) = 4$, it must be that at least one of the H_i is isomorphic to either S_4 or A_5 . In fact, one can learn even more in general about the g_i and the H_i . Another proposition in Whiston and Saxl’s paper [19] says the following:

Proposition 9. *No more than three H_i can be of the form $D_{p\pm 1}$ or G_p . If three of the H_i are of this form, then $m(G) = 3$.*

This means that when $m(G) = 4$ at least *two* of the H_i must be isomorphic to A_5 or S_4 . To proceed, it is important to understand the generating sequences of S_4 and A_5 . First of all, from Whiston's thesis [18], $m(S_n) = n - 1$ which is 3 for S_4 and since $A_5 \cong \text{PSL}(2, 5)$, $m(A_5) = 3$. Next, note the following.

Lemma 10. *Every irredundant sequence of length 3 in S_4 or A_5 must generate. As was remarked earlier, S_4 and A_5 are strongly flat.*

Proof. This follows from a careful consideration of the lattice of subgroups. The union of the sets of possible subgroups for these two groups have isomorphism classes $\{A_4, D_{10}, D_8, S_3, \mathbb{Z}_5, \mathbb{Z}_2^2, \mathbb{Z}_4, \mathbb{Z}_2, \{e\}\}$. All of these groups have $m(H) \leq 2$. \square

Since two of the H_i must be isomorphic to S_4 or A_5 , without loss of generality, suppose that H_1 and H_2 satisfy this condition. From Lemma 10, we can further deduce that $M_1 \cong M_2 \cong S_4$. The only possibilities for M_3 and M_4 by Dickson's Theorem are $S_4, D_{p\pm 1}$ and G_p . In fact, for length four sequences, this last subgroup is not possible.

Lemma 11. *Let $G = \text{PSL}(2, p)$ and $p \equiv \pm 1 \pmod{10}$ or $p \equiv \pm 1 \pmod{8}$ so that $m(G)$ can possibly be 4. Suppose that $m(G) = 4$ and let g_1, g_2, g_3, g_4 be an irredundant generating sequence of G . Without loss of generality, let $H = \langle g_2, g_3, g_4 \rangle$ be isomorphic to S_4 or A_5 and let $K = \langle g_1, g_2, g_3 \rangle$. Then, K is not isomorphic to a subgroup of G_p .*

Proof. Suppose on the contrary that $K \cong G_p$. The subgroups $L \leq K$ are isomorphic to \mathbb{Z}_p, C or $\mathbb{Z}_p \rtimes C$, where C is a subgroup of one of the isomorphic copies of $\mathbb{Z}_{(p-1)/2} \leq K$ (and is thus cyclic). Since $p > 5$, the only type which will have a potentially nontrivial intersection with H is the cyclic subgroups. Thus, to be in general position, $H \cap K$ must be cyclic. The only cyclic subgroups of S_4 and A_5 have order 2, 3 or 4, but $m(\mathbb{Z}_2) = m(\mathbb{Z}_3) = m(\mathbb{Z}_4) = 1$. Therefore, the intersection of H, K and any one of the other two subgroups corresponding to the length four irredundant generating sequence will be trivial. This contradicts the fact that these subgroups are in general position. \square

Now, we can now begin to quantify what is meant by ‘gluing’ sequences. Since H_1 and H_2 are isomorphic to either S_4 or A_5 , every length four irredundant generating sequence in G is the composite of two length three irredundant generating sequences from S_4 or A_5 . From this fact, it is clear that the next step is to study the length 3 irredundant generating sets of S_4 and A_5 . In their paper [2], Cameron and Cara determine all the length $m - 1$ irredundant generating sets of S_n except when $n = 4$ and 6. As they suggest, we approach $n = 4$ with a computation using GAP [8]:

Lemma 12. *Length three irredundant sequences (x, y, z) in S_4 and A_5 have order structure $(\text{Order}(x), \text{Order}(y), \text{Order}(z))$ equal to one of the triples below (up to permutation). Furthermore, all of these appear except $(3, 3, 3)$, which appears for A_5 but not S_4 . Since both of these groups are strongly flat and $m(G) = 3$, it must be that all of these sequences are in fact generating sequences as well.*

$$(2, 2, 2), (2, 2, 3), (3, 3, 3), (3, 2, 3)$$

Now, let’s turn our attention back to H_1 and H_2 ; g_2, g_3, g_4 is an irredundant generating sequence of length 3 in S_4 or A_5 . Thus, g_2, g_3, g_4 have orders 2 or 3 by Lemma 12. Repeating this same argument for g_1, g_3, g_4 reveals that g_1 also must have order 2 or 3. Therefore,

Proposition 13. *If $m(G) = 4$, the possible orders of elements in an irredundant generating sequence of length 4 in $\text{PSL}(2, p)$ are 2 and 3.*

Now, we will specialize to the case $p \not\equiv \pm 1 \pmod{10}$ and begin the proof of Theorem 3. The logic is broken up into four parts:

Theorem 3, Part 1 If $p \not\equiv \pm 1 \pmod{8}$, then $m(G) = 3$.

Theorem 3, Part 2a If $p \equiv \pm 1 \pmod{8}$ and $M_3 \cong M_4 \cong S_4$, then $m(G) = 3$ unless $p = 7$, in which case $m(G) = 4$.

Theorem 3, Part 2b If $p \equiv \pm 1 \pmod{8}$ and $M_3 \cong S_4$ and $M_4 \not\cong S_4$, then $m(G) = 3$.

Theorem 3, Part 2c If $p \equiv \pm 1 \pmod{8}$ and $M_3 \cong S_4$ and $M_3, M_4 \not\cong S_4$, then $m(G) = 3$.

Part 1 is proved by Whiston and Saxl's work. They prove that $m(G) = 3$ unless $p \equiv \pm 1 \pmod{8}$ or $p \equiv \pm 1 \pmod{10}$. To consider the other cases, we will need to study the properties of length three generating sequences in S_4 in more detail. First, we consider a special case of Prop. 13.

Proposition 14. *If $p \equiv \pm 1 \pmod{8}$ but $p \not\equiv \pm 1 \pmod{10}$ and $m(G) = 4$ then all the elements of an irredundant generating sequence of length of maximal length have order 2.*

Proof. First, note that

$$\langle g_i \rangle \leq (M_1 \cap M_j) \cap (M_1 \cap M_k),$$

where $1, i, j, k$ are all different. The only way for g_i to have order 3 is for 3 to divide the orders of both $L_j = M_1 \cap M_j$ and $L_k = M_1 \cap M_k$. The only subgroups of S_4 with this property are isomorphic to \mathbb{Z}_3, S_3 or A_4 . The intersection cannot be cyclic of prime order because then the H_i will not be in general position (the intersection of three will be trivial). First, suppose that both L_j and L_k are isomorphic to S_3 . Further suppose that g_i has order 3 and is in $L_j \cap L_k$. The subgroup generated by g_i is normal in L_j and L_k . However, since S_3 is maximal in S_4 , the normalizer in S_4 of $\langle g_i \rangle$ is S_3 , i.e. there is a unique S_3 which contains $\langle g_i \rangle$. This contradicts the fact that both L_j and L_k contain $\langle g_i \rangle$. We cannot have the intersection of two copies of A_4 since a given S_4 has only one of these subgroups.

All that remains is to show that one cannot have the intersection of an S_3 and a A_4 . In order for one of L_j, L_k to be A_4 , it must be that one of H_j, H_k is S_4 , since this is the only subgroup of $\text{PSL}(2, p)$ which could contain an A_4 (it is not cyclic or dihedral). Therefore, we can apply the same argument as we use for two copies of S_3 . In particular, A_4 is normal in S_4 , which is maximal in $\text{PSL}(2, p)$. Thus, there is a unique S_4 which contains the A_4 , a contradiction. Thus, g_2, g_3, g_4 have order 2 (from these arguments alone, it could be four from D_8 , but we also have shown that the orders must be 2 or 3). Clearly, we could have switched g_1 and g_2 in this argument, which shows that g_1 also has order 2. □

Later, we will need more constraints on the generating elements g_i other than just the order of the pairwise products. Using GAP and making a computation similar to Lemma 12, we can derive additional conditions.

Lemma 15. *Let g_1, g_2, g_3 be a length three irredundant generating sequence of S_4 . If the order of all the g_i is two, then*

$$[\text{Order}(g_1g_2), \text{Order}(g_2g_3), \text{Order}(g_1g_3), \text{Order}(g_1g_2g_3), \text{Order}(g_1g_2g_3g_2)]$$

is a five-tuple from the list of 13 below

$$X \equiv \left\{ [2, 3, 3, 4, 3], [2, 3, 4, 3, 4], [2, 4, 3, 3, 3], [3, 2, 3, 4, 3], [3, 2, 4, 3, 4], [3, 3, 2, 4, 3], [3, 3, 3, 4, 2], \right. \\ \left. [3, 4, 2, 3, 4], [3, 4, 4, 3, 2], [4, 2, 3, 3, 3], [4, 3, 2, 3, 4], [4, 3, 4, 3, 2], [4, 4, 3, 3, 3] \right\}$$

Let $T = \{2, 3, 4\}$. From the list in Lemma 15, one can see that given an element $Y \in T^3$, there is either no generating sequence x_1, x_2, x_3 of S_4 with the relations $(x_1x_2)^{Y[1]}, (x_1x_3)^{Y[2]}, (x_2x_3)^{Y[3]}$ or there is a unique element of X such that $X[i] = Y[i]$ for $i = 1, 2, 3$. Therefore, one can make a well-defined map $\alpha : T^3 \rightarrow X$. Let $U \subset T^3$ such that for all $Y \in U$, $\alpha(Y)$ is not empty. Then, for $Y \in U$, let

$$R_e(Y, i, j, k) = \left\{ (x_ix_jx_k)^{\alpha(Y)[4]}, (x_ix_jx_kx_j)^{\alpha(Y)[5]} \right\}.$$

Let g_1, \dots, g_n be an irredundant generating sequence of a group G and let r_1, \dots, r_m be a set of relations amongst the g_i . We will say the set of r_i is *efficient* for n if $G \cong \langle a_1, \dots, a_n | r_1, \dots, r_m \rangle$, i.e. the r_i define a presentation of G as a quotient of the free group on n generators. One can show, for example using GAP, that for $Y \in U$, the following set of relations is efficient for size 3 in S_3 so long as $\alpha(Y) \neq X[13]$.

$$\left\{ (x_ix_j)^{\alpha(Y)[1]}, (x_ix_k)^{\alpha(Y)[2]}, (x_jx_k)^{\alpha(Y)[3]}, R_e(Y, i, j, k) \right\}$$

When $\alpha(Y)$ is the last element of X , the set above is almost efficient. Therefore, we will modify R_e so that when $\alpha(Y) = X[13]$, it includes the additional relation $(x_1x_2x_1x_2x_3x_2x_3) = 1$ so that for all $Y \in U$, the set above is efficient.

The idea of the proof that follows is to construct a free group on four generators and then take a quotient which contains relations that require the

subgroup generated by triples of the free group generators in the quotient to generate S_4 . Therefore, it will be desirable to have efficient sets of relations, since the more relations that we have, the smaller the quotient of the free group will be. The goal is to show that unless the quotient group is $\text{PSL}(2, 7)$, it cannot be any other $\text{PSL}(2, p)$. The framework for this analysis will be in the context of *Coxeter Groups*, where a formalism already exists to study groups generated by n elements of order 2. A *Coxeter Group* is a group defined by the following presentation:

$$C(M) = \langle g_1, \dots, g_n | (g_i g_j)^{m_{ij}} = e \rangle,$$

where $M = \{m_{ij}\}$ is an $n \times n$ matrix such that $m_{ii} = 1$ for all $i = 1, \dots, n$. These groups have been extensively studied, but for the most part in this paper, only the notation used in describing these groups will be used - as a mechanism for book-keeping. Since all of the elements of an irredundant generating sequence of length four in $G = \text{PSL}(2, p)$ when $p \not\equiv \pm 1 \pmod{10}$ must have order 2, it is clear that G is a quotient of $C(M)$ for some (possibly not unique) M . Recall that $\langle g_1, g_3, g_4 \rangle$ and $\langle g_1, g_3, g_4 \rangle$ are isomorphic to S_4 . Therefore, there are restrictions on what M can be for G a quotient of $C(M)$. In what follows, Theorem 3, Parts 2a, 2b and 2c will be studied by examining the possibilities for M . Applying additional knowledge about length three generating sequences of S_4 will then lead to the final conclusion. In the proof of Part 2a, every triple of the g_i generates an isomorphic copy of S_4 . Define $C^a(M)$ to be the following application of the efficient relations:

$$C^a(M) = \langle x_1, x_2, x_3, x_4 | (x_i x_j)^{m_{ij}}, R_e((m_{ij}, m_{ik}, m_{jk}), i, j, k) \rangle.$$

In the proof of Part 2b, all of the triples except $\{g_1, g_2, g_3\}$ generate an isomorphic copy of S_4 . For this case, define

$$C^b(M) = \langle x_1, x_2, x_3, x_4 | (x_i x_j)^{m_{ij}}, R_e((m_{23}, m_{24}, m_{34}), 2, 3, 4), \\ R_e((m_{13}, m_{14}, m_{34}), 1, 3, 4), R_e((m_{12}, m_{14}, m_{24}), 1, 2, 4) \rangle.$$

Finally, for Part 3b, only H_1 and H_2 are isomorphic to S_4 and so a maximal application of the S_4 relations leads us to define

$$C^c(M) = \langle x_1, x_2, x_3, x_4 | (x_i x_j)^{m_{ij}}, R_e((m_{23}, m_{24}, m_{34}), 2, 3, 4), R_e((m_{13}, m_{14}, m_{34}), 1, 3, 4) \rangle$$

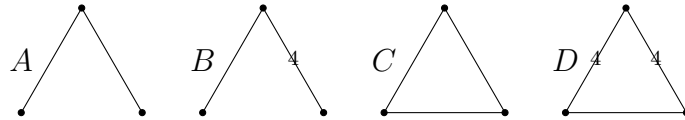
To ease notation, instead of dealing with the matrices M , consider the instead corresponding *Coxeter diagrams*. In a Coxeter diagram $D(M)$, elements i are generated with points and lines between points i and j represent m_{ij} . If no line exists between points labeled i and j , then $m_{ij} = 2$. If there is a solid line, then $m_{ij} = 3$. For all other m_{ij} , there will be a solid line with the order drawn on top of the line. Since the largest order of elements in S_4 is 4 and conditions involving orders of elements in this symmetric group are the only relations we will impose, the only possibilities for a piece of the Coexeter diagram for $C(M)$ are

$$\bullet \quad \bullet \quad \bullet \text{---} \bullet \quad \bullet \text{---} 4 \text{---} \bullet$$

To further ease the notation, we will abbreviate two diagrams with one:

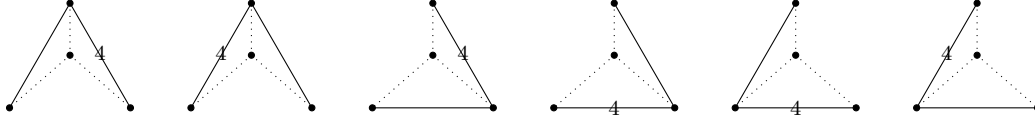
$$\bullet \text{---}(4)\text{---} \bullet = \left\{ \bullet \text{---} 4 \text{---} \bullet, \bullet \text{---} \bullet \right\}$$

Any diagram with a dotted line will denote represent the three diagrams where any one of the three possible connectors is substituted for the dotted line. We will say two diagrams are *equivalent* if for the associated matrices M, N , $C^x(M) \cong C^x(N)$ where $x = a, b, c$ depending on which part of the main theorem we are considering. To begin, note that every length four irredundant generating sequence is built from a length three generating sequence of S_4 . Up to the permutation of the three elements, the only four diagrams corresponding to length three irredundant generating sequences of S_4 are

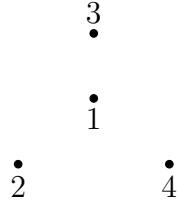


Therefore, in considering cases Part 2a, Part 2b and Part 2c it suffices to study extensions of these four diagrams. To begin, consider case a in which all the g_i are in an isomorphic copy of S_4 . In this case, when one more node is added to the above diagrams, there are three possible lines that can

be drawn between this new node and each of the existing nodes: no line, a solid unadorned line and a line with the number 4. This means that there are $4 \times 27 = 108$ possible diagrams. Note that we do not need to consider diagrams which are built from rotations or reflections of A, B, C or D in the proof of Part 2a since such diagrams are equivalent to the ones we will consider. For example, the following diagrams are equivalent in Part 2a:

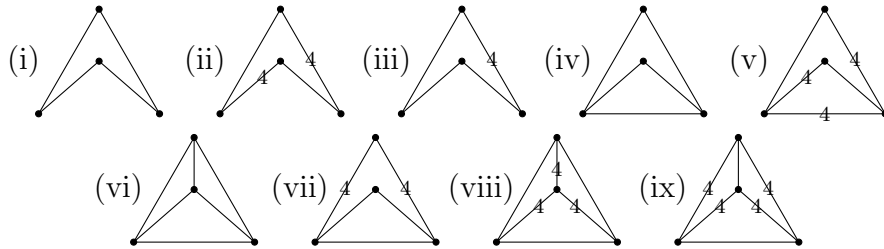


However, when considering sub-diagrams, we cannot enforce that they look exactly like A, B, C or D - instead they must be rotations or reflections of these basic diagrams. Associate to g_1, g_2, g_3, g_4 the labeled diagram below:

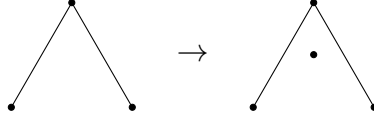


In proving Part 2a, we will have four cases. These cases will correspond to the sub-diagram formed by the points $(2, 3, 4)$ taking the form A, B, C and D . Then, to eliminate many of the diagrams, we will enforce the conditions that the sub-diagrams formed by the points $(1, 2, 3)$, $(1, 2, 4)$ and $(1, 3, 4)$ must be a rotation or reflection of A, B, C or D . This will reduce the number of diagrams to a small list. From this list, we will apply the efficient conditions by considering $C^a(M)$. It is possible to combine these steps into one, which has been done with a computer program. However, to explicitly describe all the logic, the two-step process is recorded here.

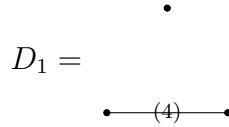
Proposition 16. *For Part 2a, the only distinct extensions of the four base diagrams A, B, C and D are below.*



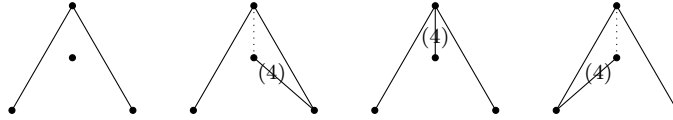
Proof. It is easiest to analyze the diagrams by fixing a base diagram and then considering all the possible ways to add the fourth node. First, attempt to add a node the diagram A .



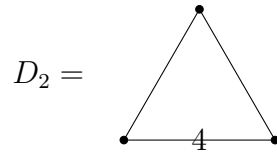
First, we consider the diagrams which are forbidden because they contain a sub-diagram D_1 which has the graphical form given below.



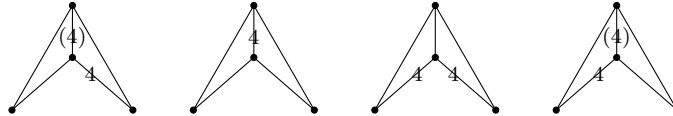
These 15 diagrams are as follows.



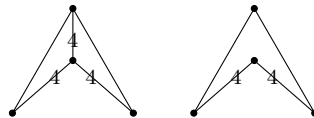
Next, we can rule out the remaining diagrams which have a sub-diagram D_2 of the form



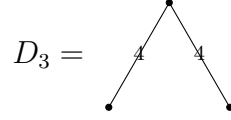
These 6 diagrams are displayed below.



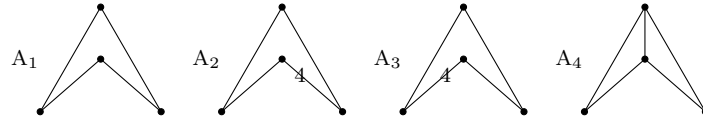
Finally, we exclude the following 2 diagrams.



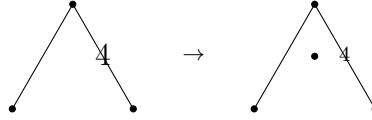
These are not allowed because they contain the forbidden sub-diagram D_3 .



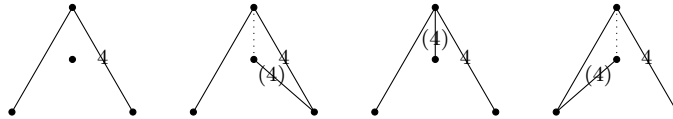
There are $27 - 23 = 4$ remaining diagrams, which are allowed. These diagrams have been labeled $A_i, i = 1, 2, 3, 4$.



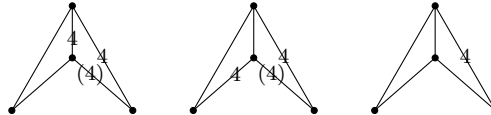
However, it is clear that A_2 is equivalent to A_3 so there are 3 distinct extensions of A that contribute to the proposition. Now, we add a node to the diagram B .



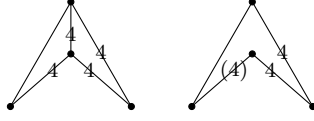
As before, we begin by eliminating the diagrams which contain D_1 as a sub-diagram. These 15 diagrams are below. Clearly, there is a one-to-one relation between these and the ones eliminated by D_1 sub-diagrams in the first case.



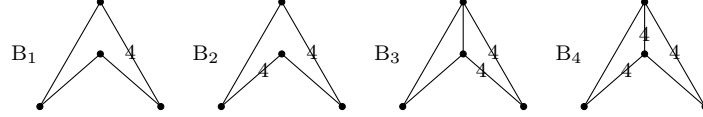
Next, we eliminate remaining diagrams which contain D_2 as a sub-diagram. These 5 diagrams are displayed below.



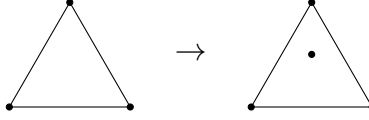
Finally, we exclude the following 3 remaining diagrams which contain D_3 as a sub-diagram.



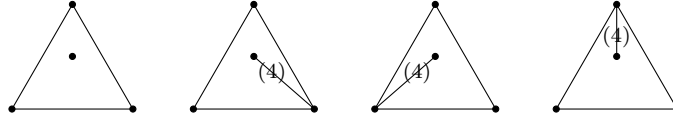
The remaining $27 - 24 = 4$ diagrams are then labeled $B_i, i = 1, 2, 3, 4$.



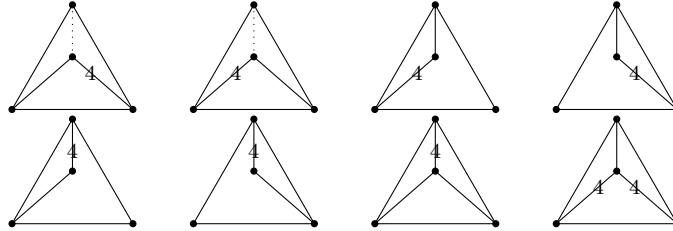
This brings the total number of distinct allowed diagrams to six, since B_1 is equivalent to A_2 . The next step is to extend the base diagram C .



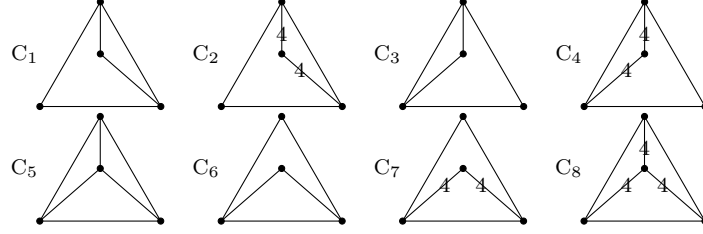
The 7 diagrams which contain D_1 as a sub-diagram are shown below.



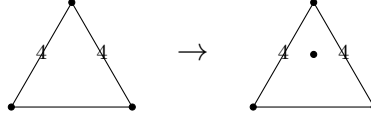
As in the previous cases, we next proceed to eliminate D_2 as a sub-diagram. For extensions of C , there are 12 such diagrams.



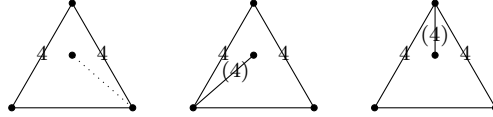
The remaining diagrams are all allowed - the condition that no remaining diagram contain D_3 as a sub-diagram does not further reduce the list. The allowed $27 - 19 = 8$ extensions of C are named $C_i, i = 1, \dots, 8$.



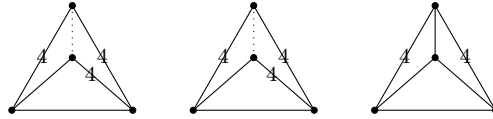
However, the following two sets of diagrams are equivalent: $\{C_1, C_3, C_6\}$ and $\{C_2, C_4, C_7\}$. Therefore, this list collapses to three distinct diagrams. In fact, C_1 is equivalent to A_4 and C_2 is equivalent to B_3 so the total number of diagrams so far is now at 8. We are now ready for the last case - extending the base diagram D .



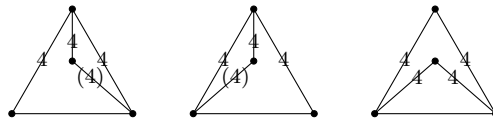
There is a 1-1 correspondence between the D extensions containing D_1 sub-diagrams and the C extensions contain D_1 sub-diagrams. The 7 eliminated D extensions are below.



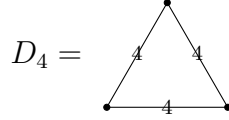
There are also 7 remaining D extensions which contain D_2 as a sub-diagram.



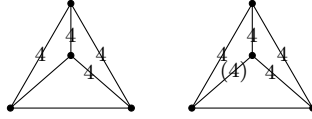
Unlike for C extensions, there are remaining diagrams which contain D_3 as a sub-diagram. The 5 such diagrams are listed below.



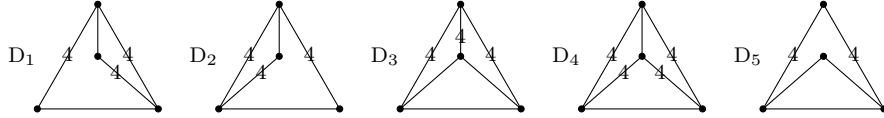
In the extensions of A , B and C , these conditions were enough to rule out diagrams. However, for D extensions, there are remaining diagrams which contain a sub-diagram denoted D_4 which is not permitted.



There are three remaining sub-diagrams which contain D_4 .



After eliminating extensions with sub-diagrams of the form D_i , $i = 1, 2, 3, 4$ the remaining diagrams are all allowed. These $27 - 22 = 5$ diagrams are labeled D_i , $i = 1, \dots, 5$.



Only one of these diagrams is new - D_4 . D_1 is equivalent to D_2 which is equivalent to B_4 . The diagram D_5 is equivalent to B_3 . Finally, D_3 is equivalent to C_8 . Therefore, the distinct 9 allowed diagrams are equivalent to $A_1, A_2, A_4, B_2, B_3, B_4, C_5, C_8$ and D_4 .

□

Now, imposing further conditions on the diagrams from Prop. 16 will allow us to prove Part 2a of the theorem.

Theorem 17 (Main Theorem Part 2a). *If $p \equiv \pm 1 \pmod{8}$ and $M_3 \cong M_4 \cong S_4$, then $m(G) = 3$ unless $p = 7$, in which case $m(G) = 4$.*

Proof. All that remains is to decide if any $\text{PSL}(2, p)$ can be a quotient of $C^a(M)$ for an M associated to one of the diagrams in Prop 16. There are two properties that we will use to make this determination: order and solvability. After $\text{PSL}(2, 7)$, the next smallest G is $\text{PSL}(2, 17)$, which has order 2448. If $|C^a(M)| < 2448$, then $\text{PSL}(2, 7)$ is the only possible quotient. Furthermore, if $C^a(M)$ is solvable, then it is not possible for G to be a quotient since all

non-trivial G in Part 2a are simple. This later condition can be used to immediately eliminate diagram (i) from Prop 16. The corresponding $C(M)$ is isomorphic to the Euclidean Coxeter group \tilde{A}_3 [1], which is isomorphic to $\mathbb{Z}^3 \rtimes S_4$. Since this group is solvable and G is simple, G cannot be a quotient of A . For the rest of the groups, the strategy will be to show that $C^a(M)$ is too small. For this, we use the Todd-Coxeter (TC) Algorithm [16], which can determine the order of a group given by a presentation in some cases. The results of this are in Table 1.

Prop. 16 Diagram	$ C^a(M) $	Prop. 16 Diagram	$ C^a(M) $
ii	168	vi	120
iii	168	vii	96
iv	192	viii	24
v	1	ix	1

Table 1: Size of $C^a(M)$ for the matrices M associated to the diagrams in Prop. 16.

From Table 1, we can see that none of the possible groups are big enough to be a G with $p > 7$. A computation for $\text{PSL}(2, 7)$ shows that it does have a length four irredundant generating sequence such that each triple generates an isomorphic copy of S_4 . Such sequences correspond to diagrams ii and iii in Table 1.

□

Now, we proceed to Part 2b, where M_4 is isomorphic to a dihedral group. Since all the other $M_i \cong S_4$, it is still true that all the pairwise products of the g_i have orders 2, 3 or 4 (each pair sits inside an isomorphic copy of S_4). However, in Part 2a, we had four criteria for the Coxeter diagrams, one for each triple of elements. In Part 2b, M_4 is not isomorphic to S_4 and so we lose one condition. Therefore, before writing down diagrams, we will establish a new criteria.

Lemma 18. *Let $K_1 = H_1 \cap H_4$, $K_2 = H_2 \cap H_4$ and $K_3 = H_3 \cap H_4$. If $H_3 \cong S_4$ and H_4 is dihedral, then no two of the K_i can be isomorphic to S_3 .*

Proof. First, we observe that if a dihedral group has a cyclic subgroup of order 3 or 4, then it is unique. This is because such a subgroup sits inside the cyclic subgroup of index 2 in the dihedral group. Cyclic groups have precisely one subgroup of each divisor of their order and so this subgroup

must be unique. Suppose that $K_1 \cong K_2 \cong S_3$. We know that there is a unique subgroup of H_4 of order 3 and so it must be in both H_1 and H_2 . Therefore, $H_1 \cap H_2 \cap H_4$ must have order 3 (it cannot have order 6 because then the H_i would not be in general position). However,

$$\langle g_3 \rangle \leq H_1 \cap H_2 \cap H_4$$

and so this would mean that g_3 has order 3 (or one), a contradiction. Therefore, no two of the K_i can be isomorphic to S_3 . □

Corollary 19. *No two of $Order(g_1g_2)$, $Order(g_1g_3)$, $Order(g_2g_3)$ can be 3*

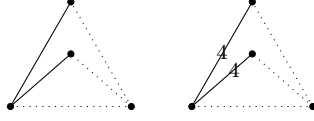
Proof. By the lemma, no two of the K_i can be isomorphic to S_3 . This means that no two of $\langle g_1, g_2 \rangle$, $\langle g_1, g_3 \rangle$ and $\langle g_2, g_3 \rangle$ can be isomorphic to S_3 . Since all the g_i have order 2, this means that no two of $Order(g_1g_2)$, $Order(g_1g_3)$, $Order(g_2g_3)$ can be 3. □

A similar result is true for D_8 .

Proposition 20. *No two of $Order(g_1g_2)$, $Order(g_1g_3)$ and $Order(g_2g_3)$ can be four.*

Proof. Suppose without loss of generality that $Order(g_1g_2) = Order(g_1g_3) = 4$. Then, $H_3 \cap H_4 \cong H_2 \cap H_4 \cong D_8$. To see this, note for example that $\langle g_1, g_2 \rangle \leq H_3 \cap H_4$, but $\langle g_1, g_2 \rangle \cong D_8$, which is maximal and so this is equality. Next, note that H_4 has a unique cyclic group of order 4 which is in common to both of $H_3 \cap H_4$ and $H_2 \cap H_4$. Therefore, $H_2 \cap H_3 \cap H_4$ is cyclic of order 4 (it cannot be all of the dihedral group since then the H_i would not be in general position). In $H_2 \cap H_4$, the cyclic group of order four is $\langle g_1g_3 \rangle$ and in $H_3 \cap H_4$, the cyclic group of order four is $\langle g_1g_2 \rangle$. The fact that these are the same means that $g_1g_2 = g_1g_3$ or $g_1g_2 = (g_1g_3)^3$. Then, we can write $g_2 = g_1(g_1g_3)^x$, where $x = 1$ or 3 . This contradicts the fact that the set of g_i is irredundant. □

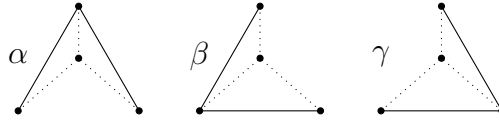
In terms of diagrams, this will mean that sub-diagrams that look like the following will be eliminated.



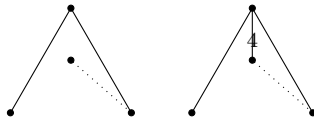
Now, we have enough criteria to reduce the number of diagrams to a manageable size. There are still many more diagrams than we encountered in Part 2a, so the analogy of Prop 16 will be broken into four: one for each flavor of base diagram A, B, C or D . This is because the broken symmetry in the diagram requires us to consider not only the original base diagrams, but also their rotations and reflections.

Proposition 21 (Extensions of the Base Diagram A). *Given the same conditions in Theorem 3 Part 2b, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram A .*

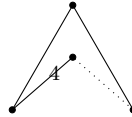
Proof. There are three possibilities for the sub-diagram generated by nodes $(2, 3, 4)$:



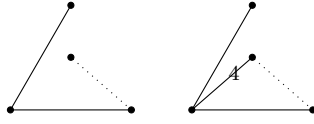
We first begin with α . With the new criteria for Part 2b, Cor. 19 and the constraint that $(g_2g_3)^3 = 1$ the only possibilities for the orders of (g_1g_2) and (g_1g_3) are $(2, 2), (2, 4)$ and $(4, 2)$. Note that all the following diagrams are excluded because the sub-diagram formed by the nodes $(1, 2, 4)$ is not a rotation or reflection of A, B, C or D .



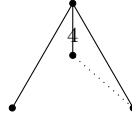
The remaining diagrams are as follows.



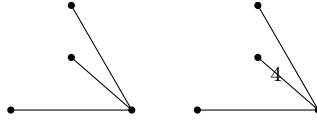
The only way for the sub-diagram generated by the nodes $(1, 2, 4)$ to be of the form A, B, C or D is for the dotted line to be a solid line. Call this diagram A_1 for later analysis. Next, we consider β . Cor. 19 and the constraint that $(g_2g_3)^3 = 1$ apply the same as in the previous case to show that the only possibilities for the orders of (g_1g_2) and (g_1g_3) are $(2, 2)$, $(2, 4)$ and $(4, 2)$. The following diagrams are excluded because the sub-diagram formed by one of $(1, 2, 4)$ or $(1, 3, 4)$ would not be a rotation or reflection of A, B, C or D .



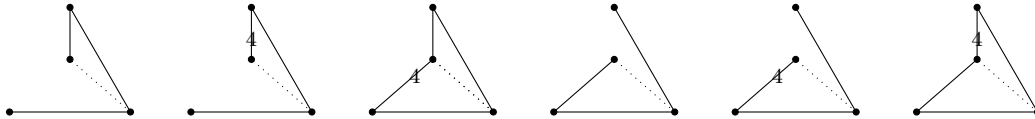
The remaining 3 diagrams are given below.

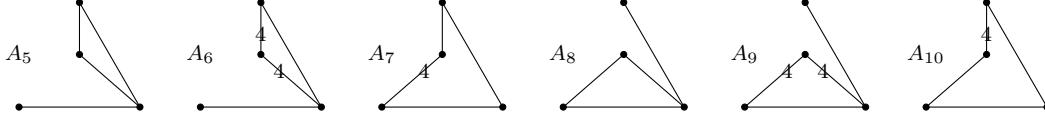


Once again, the only way for the sub-diagram generated by the nodes $(1, 2, 4)$ to be of the form A, B, C or D is for the dotted line to be a solid line. Call this diagram A_2 for later analysis. Finally, we consider γ . Cor. 19 and the constraint that $(g_2g_3)^2 = 1$ require that the orders of (g_1g_2) and (g_1g_3) be one of $\{(2, 2), (2, 3), (3, 2), (2, 4), (4, 2), (3, 4), (4, 3)\}$. If the order pair is $(2, 2)$, then for the sub-diagram $(1, 2, 4)$ to be one of A, B, C or D , only the following diagrams are allowed.



Label these A_3 (left) and A_4 (right) for later analysis. For each of the remaining pairs of orders for (g_1g_2) and (g_1g_3) , there is only one allowed diagram based on the criteria that all the non $(1, 2, 3)$ sub-diagrams be one of A, B, C or D . This is illustrated below. The first row is the generic set of diagrams and the second row show the single allowed diagram.





Now, we are ready to apply the efficient relations and use the Todd-Coxeter algorithm to deduce the size of $C^b(M)$. The results of this are in Table 2.

Diagram	$ C^b(M) $	Diagram	$ C^b(M) $
A_1	1344	A_6	24
A_2	1344	A_7	1344
A_3	192	A_8	120
A_4	96	A_9	24
A_5	120	A_{10}	1344

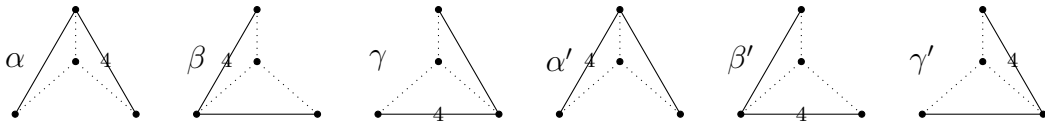
Table 2: Size of $C^b(M)$ for the matrices M associated to the diagrams A_i .

Table 2 shows that for $p > 7$, G cannot be a quotient of $C^b(M)$ for M associated with an A extension. In fact, a computation for $G = \text{PSL}(2, 7)$ shows that the only structure of length four irredundant generating sequences is for $M_i \cong S_4$, $i = 1, 2, 3, 4$.

□

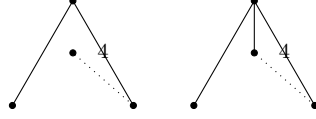
Proposition 22 (Extensions of the Base Diagram B). *Given the same conditions in Theorem 3 Part 2b, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram B .*

Proof. There are six possibilities for the sub-diagram generated by nodes $(2, 3, 4)$.

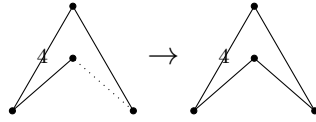


The set of diagrams α have the same restrictions from Cor. 19 as the corresponding set of diagrams in the analysis of base A extensions. In particular,

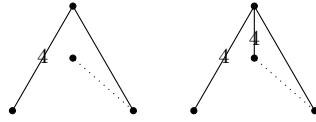
since the order of (g_2g_3) is 3 the only possibilities for the orders of (g_1g_2) and (g_1g_3) are $(2, 2)$, $(2, 4)$ and $(4, 2)$. This excludes the following diagrams.



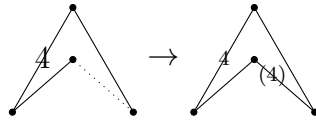
Of the remaining diagrams (shown below on the left) only one is permissible given the constraints on the S_4 sub-diagrams (below, right).



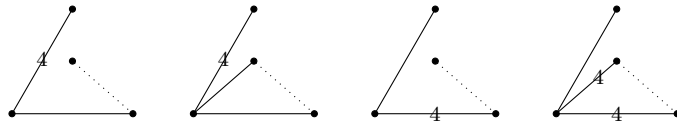
Let the matrix M_1 correspond to the permitted diagram shown above. The TC algorithm produces $|C^b(M_1)| = 168$, too small for a G to be a quotient for $p > 7$. There is a similar story for α' . The order of (g_2g_3) is four so the only possibilities for the orders of (g_1g_2) and (g_1g_3) are $(2, 2)$, $(2, 3)$ and $(3, 2)$. This excludes the following diagrams.



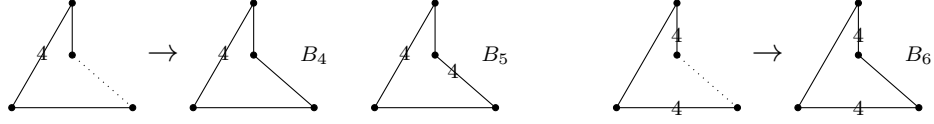
Of the remaining diagrams two are permissible given the constraints on the S_4 sub-diagrams.



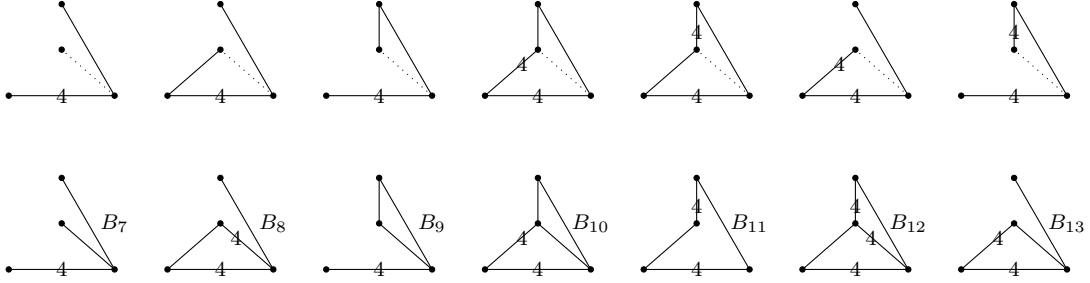
Let the matrices M_2, M_3 correspond to the permitted diagram in the middle and right, respectively. The TC algorithm produces $|C^b(M_2)| = 1344$, $|C^b(M_3)| = 168$, once again too small for a G to be a quotient for $p > 7$. The analysis on β and β' proceeds analogously to α and α' . Cor. 19 and the constraint on (g_2g_3) eliminates the following diagrams.



Of the remaining diagrams, the S_4 sub-diagram constraints leaves only three permissible extensions.



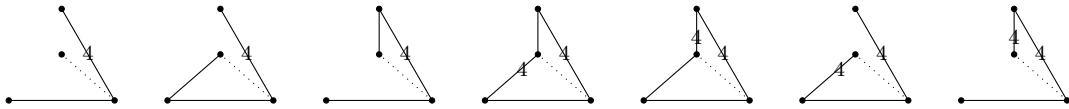
If M_i is the matrix associated to B_i , we can compute $|C^b(M_i)|$ using the TC algorithm. This produces $|C^b(M_4)| = 1344$, $|C^b(M_5)| = 168$ and $|C^b(M_6)| = 168$ and so these cases are eliminated. For the remaining bases, there are only a small number of possible extensions. In the diagram that follows, the top row show the set of remaining cases and the bottom rows list all allowable diagrams, taking into account the restrictions from Cor. 19 and the sub-diagram criteria. First, γ diagrams.

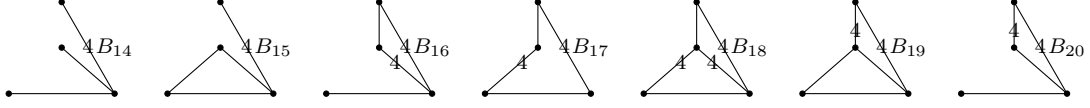


The results of applying the TC algorithm to determine order are in Table 3. We now repeat this analysis for γ' diagrams.

Diagram	$ C^b(M) $	Diagram	$ C^b(M) $
B_7	96	B_{11}	168
B_8	1	B_{12}	1
B_9	24	B_{13}	24
B_{10}	96		

Table 3: Size of $C^b(M)$ for the matrices M associated to the diagrams $B_i, i = 7, \dots, 13$.





The results of applying the TC algorithm to determine order are in Table 4.

Diagram	$ C^b(M) $	Diagram	$ C^b(M) $
B_{14}	96	B_{18}	1
B_{15}	24	B_{19}	96
B_{16}	1	B_{20}	24
B_{17}	168		

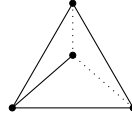
Table 4: Size of $C^b(M)$ for the matrices M associated to the diagrams $B_i, i = 14, \dots, 20$.

Tables 3 and 4 conclude the proof for extensions of B .

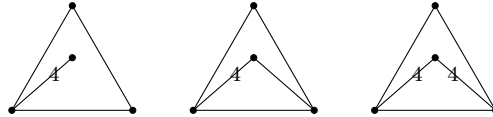
□

Proposition 23 (Extensions of the Base Diagram C). *Given the same conditions in Theorem 3 Part 2b, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram C .*

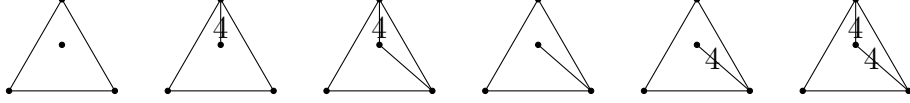
Proof. Since the order of g_2g_3 is three, Cor. 19 limits the only possibilities for the orders of (g_1g_2) and (g_1g_3) to $(2, 2)$, $(2, 4)$ and $(4, 2)$. This eliminates a third of all possible diagrams.



If instead of the the inner solid line, the diagram had a solid line with a four, there are three possible diagrams.



The first two of these diagrams are eliminated by S_4 sub-diagram criteria. For the third diagram, $|C^b(M)| = 96$. If the order of g_1g_2 is two, there are six diagrams.

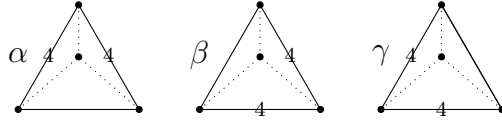


The first three of these diagrams are forbidden by S_4 sub-diagram criteria. For the remaining three, $|C^b(M)| = 120, 24$ and 96 , respectively.

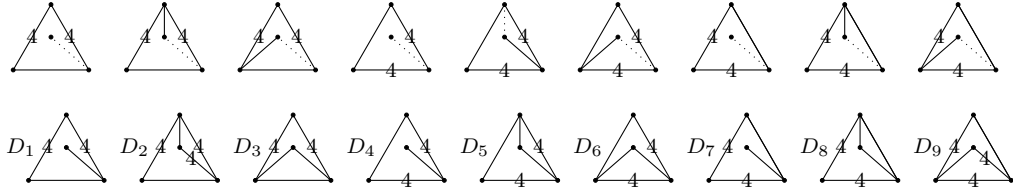
□

Proposition 24 (Extensions of the Base Diagram D). *Given the same conditions in Theorem 3 Part 2b, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram D .*

Proof. There are three possibilities for the sub-diagram generated by nodes $(2, 3, 4)$:



From Cor. 19 and the limits on the orders on (g_1g_2) and (g_1g_3) , each of α, β and γ have only three allowed sets of diagrams. Below in the first row is the list of sets of diagrams and below in the second row are the allowed diagrams after applying S_4 sub-diagram criteria. For each set, it turns out there is only one allowed diagram by the symmetric group sub-diagram criteria.



The results of applying the TC algorithm to determine order are in Table 6. Table 6 concludes the proof for extensions of D .

□

Propositions 21, 22, 23 and 24 then can be summarized as follows.

Diagram	$ C^b(M) $	Diagram	$ C^b(M) $
D_1	24	D_6	1
D_2	1	D_7	24
D_3	96	D_8	96
D_4	1	D_9	1
D_5	1		

Table 5: Size of $C^b(M)$ for the matrices M associated to the diagrams $D_i, i = 1, \dots, 9$.

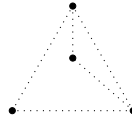
Theorem 25 (Main Theorem Part 2b). *If $p \equiv \pm 1 \pmod{8}$ and $M_3 \cong S_4$ and $M_4 \not\cong S_4$, then $m(G) = 3$.*

Finally, in order to apply the Todd-Coxeter strategy to the last case of the theorem, we will once again need to establish some more sub-diagram criteria, since Part 2c has two fewer conditions than Part 2a. For this, we have the following lemma.

Lemma 26. *If M_3 and M_4 are dihedral groups, then their intersection is isomorphic to \mathbb{Z}_2^2 .*

Proof. Since the only subgroups of dihedral groups are cyclic or dihedral, $H = M_3 \cap M_4$ must be cyclic or dihedral. Suppose that H is cyclic and let K be an index two cyclic subgroup of M_3 . H cannot have order 2 because the M_i are in general position. Therefore, $H \leq K$. However, every subgroup of a cyclic subgroup is characteristic and so $H \leq M_3$. Since M_3 is maximal in G , it must be that $M_3 = N_G(H)$. However, the same argument shows that $M_4 = N_G(H)$. Therefore, $M_3 = M_4$, a contradiction. Thus, H must be dihedral. Let $L \leq H$ be the cyclic subgroup of index 2. By our previous discussion, if $|L| > 2$, there would be a unique dihedral group in G which contains L , a contradiction. Therefore, we must have $|L| = 2$ and so $H \cong \mathbb{Z}_2^2$. \square

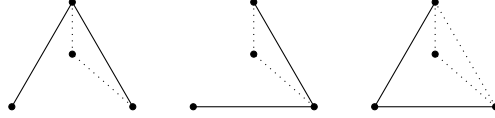
In terms of sub-diagrams, Lemma 26 means that for Part 2c, all the diagrams will have the following form.



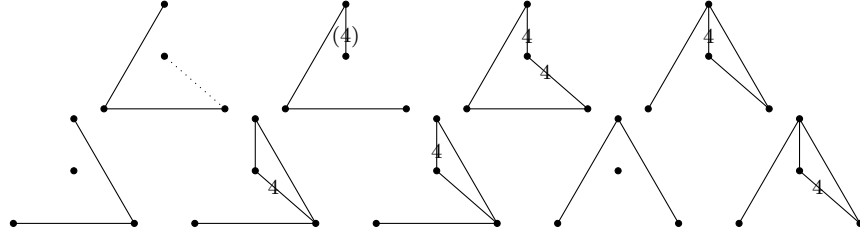
As with Part 2b, we will proceed by breaking up the proof by base diagram. However, instead of starting with A and moving towards D , we will go A, C, D and then end with B . This is because A, C and D can be easily eliminated using the same strategy as in the other cases. However, B will require additional work, which we will save for the very end of the proof of the theorem. As we loop over the base diagrams for the sub-diagram $(2, 3, 4)$, the only other criteria that we have besides Lemma 26 is the S_4 criteria for the sub-diagram $(1, 3, 4)$.

Proposition 27 (Extensions of the Base Diagram A). *Given the same conditions in Theorem 3 Part 2c, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram A .*

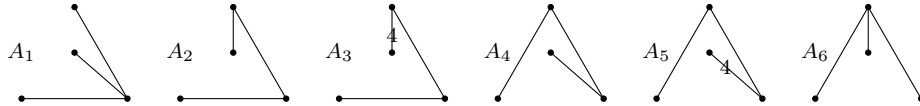
Proof. There are three types of diagrams that are possible with A extensions.



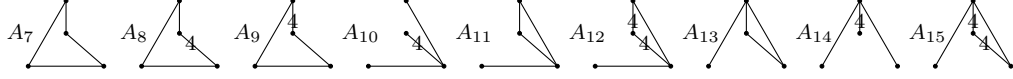
Each of these types includes 9 distinct diagrams and therefore, there are 27 total A extensions. Twelve of these fail the sub-diagram S_4 criteria.



Next, consider the following set of 6 diagrams. These are finite Coxeter groups [5] and so no further restrictions are required.



The diagrams A_1 and A_6 correspond to the Coxeter group D_4 , which has order 192 [5]. A_2 and A_4 correspond to the Coxeter group A_4 , which has order 120. The remaining diagrams, A_3 and A_5 correspond to the Coxeter Group BC_4 , which has order 384. There are then $27 - 18 = 9$ remaining diagrams.



The diagram A_7 corresponds to the Coxeter group \tilde{A}_3 [1], which as we noted in the proof of Part 2a is solvable. The rest of the A_i are eliminated by order considerations from the TC algorithm, summarized in Table 6.

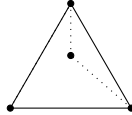
Diagram	$ C^c(M) $	Diagram	$ C^c(M) $
A_8	1344	A_{12}	24
A_9	1344	A_{13}	120
A_{10}	192	A_{14}	192
A_{11}	120	A_{15}	24

Table 6: Size of $C^c(M)$ for the matrices M associated to the diagrams $A_i, i = 8, \dots, 15$.

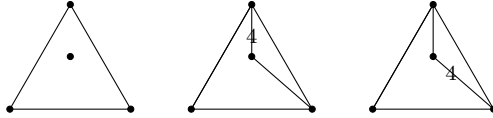
□

Proposition 28 (Extensions of the Base Diagram C). *Given the same conditions in Theorem 3 Part 2c, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram C .*

Proof. There are only nine possible diagrams.



Three of these diagrams are eliminated by S_4 sub-diagram criteria.



The remaining six diagrams are below.

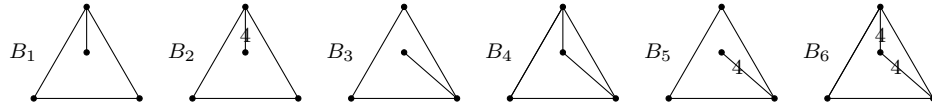


Diagram	$ C^c(M) $	Diagram	$ C^c(M) $
B_1	120	B_4	192
B_2	24	B_5	24
B_3	120	B_6	192

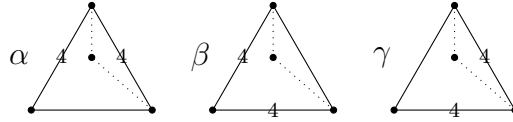
Table 7: Size of $C^c(M)$ for the matrices M associated to the diagrams $B_i, i = 1, \dots, 6$.

These B_i are eliminated by order considerations from the TC algorithm, summarized in Table 7.

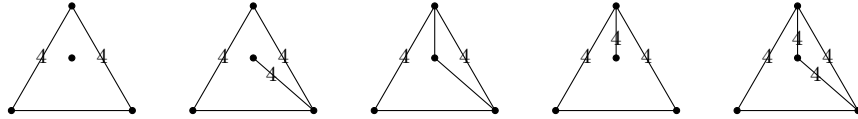
□

Proposition 29 (Extensions of the Base Diagram D). *Given the same conditions in Theorem 3 Part 2c, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram D .*

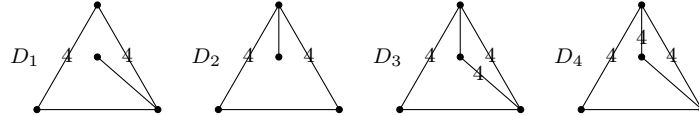
Proof. There are three types of diagrams that are possible with C extensions.



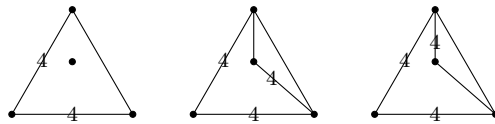
Five of the α diagrams are eliminated by S_4 sub-diagram criteria.



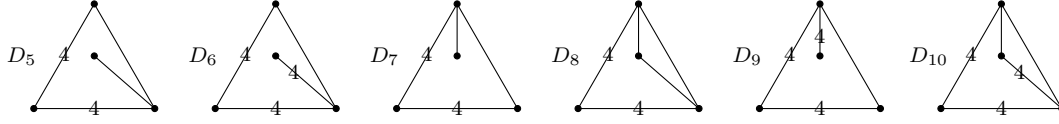
The remaining α diagrams are below.



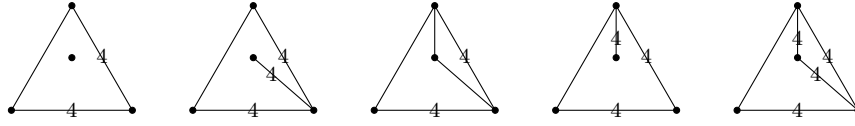
Of the β diagrams, three are eliminated by S_4 sub-diagram criteria.



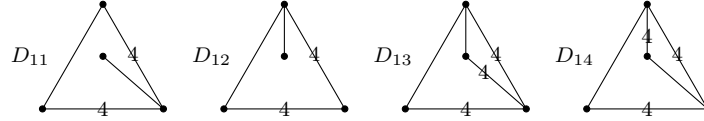
The six permitted β diagrams are shown below.



Finally, we consider the γ diagrams. Five of these diagrams are eliminated by S_4 sub-diagram criteria.



The γ diagrams which are allowed are as follows.



From the three cases α, β and γ , all diagrams have been eliminated from order considerations using the TC algorithm, summarized in Table 9.

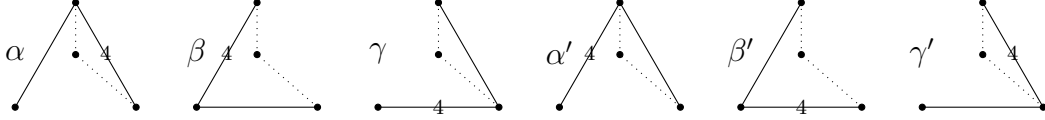
Diagram	$ C^c(M) $	Diagram	$ C^c(M) $
D_1	24	D_8	192
D_2	1	D_9	96
D_3	1	D_{10}	192
D_4	96	D_{11}	1
D_5	24	D_{12}	24
D_6	96	D_{13}	96
D_7	24	D_{14}	1

Table 8: Size of $C^c(M)$ for the matrices M associated to the diagrams $D_i, i = 1, \dots, 14$.

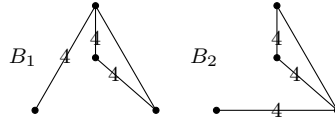
□

Proposition 30 (Extensions of the Base Diagram B). *Given the same conditions in Theorem 3 Part 2c, no length four irredundant generating sequence can be built as an extension of the length three sequences in S_4 associated with the base diagram B .*

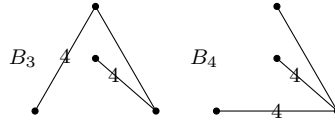
Proof. There are six possible sets of diagrams, each with 9 diagrams, for a total of 54 diagrams to consider.



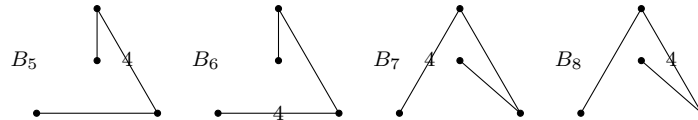
First, note that any diagram with only two solid lines is not allowed by the S_4 criteria for the sub-diagram (1,3,4). There are 6 such diagrams - lowering the total number to 48. Now, suppose that both dotted lines in the above diagrams are solid and have a four. Such diagrams are ruled out by the S_4 criteria unless the line connecting 3 and 4 is a solid unadorned line. There are two such diagrams.



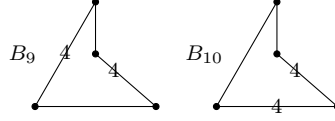
Now, we are left with 42 diagrams. Next, consider diagrams in which the line connecting nodes 1 and 4 is a solid line with a four and there is no line connecting nodes 1 and 3. The only way for such diagrams to be allowed by the sub-diagram criteria is for the line connecting nodes 3 and 4 to be a solid unadorned line. This results in two allowed diagrams.



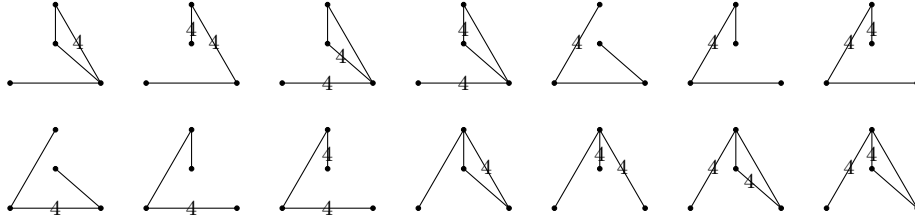
This observation now has lowered the total number of diagrams to 36. Now, consider the allowed diagrams which correspond to finite Coxeter groups.



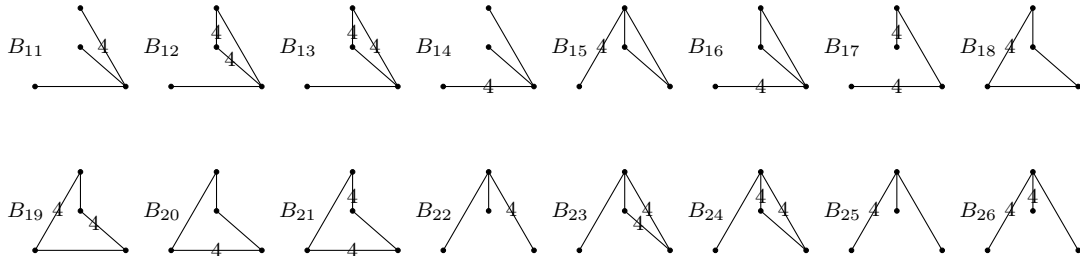
The diagrams B_5 and B_6 correspond to the Coxeter group F_4 , which has order 1152. The diagrams B_7 and B_8 correspond to the Coxeter group BC_4 , which has order 384. Let the diagrams B_9 and B_{10} be as below.



These two diagrams are allowed by all the criteria. However, the TC algorithm does not terminate in a ‘reasonable’ amount of time. Therefore, one needs another method to rule them out. We will return to these diagrams at the end. Of the 30 remaining diagrams, 14 are ruled out by the sub-diagram criteria and 16 are permitted. First, what follows is list of the excluded diagrams.



Next, below is a list of the permitted diagrams with labels for later analysis.



Except for B_9 and B_{10} , TC algorithm rules out all of the B_i , summarized in Table 9.

Now, let us return to B_9 and B_{10} . First, we observe that these diagrams are equivalent, since if we send $g_1 \mapsto g_2$ B_9 will become B_{10} . This exchange is permitted because g_1, g_2 are in the intersection of the dihedral groups and so this does not ruin the group structure of the H_i . Even though the TC procedure does not terminate in a reasonable time to determine the size of $C^c(M)$, it can be used to investigate subgroups of finite index. Let M denote the Coxeter matrix associated to B_{10} and let $x, y, z \in C^c(M)$ be such that

Diagram	$ C^c(M) $	Diagram	$ C^c(M) $
B_1	96	B_{17}	96
B_2	96	B_{18}	1344
B_3	96	B_{19}	1344
B_4	192	B_{20}	1344
B_{11}	96	B_{21}	1344
B_{12}	1	B_{22}	96
B_{13}	24	B_{23}	24
B_{14}	192	B_{24}	1
B_{15}	24	B_{25}	192
B_{16}	24	B_{26}	192

Table 9: Size of $C^c(M)$ for the matrices M associated to the diagrams $B_i, i = 1, 2, 3, 4, 11, 12, \dots, 26$.

$x = g_4g_1g_4g_2, y = g_1g_4g_2g_4$ and $z = g_3g_4g_1g_4g_2g_3$, where here g_i denotes the image of the i^{th} generator in $C^c(M)$. Then, the TC procedure allows us to show that $\langle x, y, z \rangle \leq C^c(M)$ has index 24. Furthermore, the algorithm enumerates the cosets and so we can further deduce from the procedure that $\langle x, y, z \rangle \trianglelefteq C^c(M)$ and the quotient is isomorphic to S_4 . The final observation is that $\langle x, y, z \rangle$ is commutative. Showing this property is a routine application of the efficient relations. The details of the computation are in Appendix B. Since $\langle x, y, z \rangle$ is abelian and the quotient is solvable, it must be that $C^c(M)$ is solvable and so G cannot be a quotient. \square

Propositions 27, 30, 28 and 29 now complete the proof of the Main Theorem.

Theorem 31 (Main Theorem Part 2c). *If $p \equiv \pm 1 \pmod{8}$ and $M_3, M_4 \not\cong S_4$, then $m(G) = 3$.*

4. $\text{PSL}(2, p)$ and the Replacement Property

While it is not known in general if $G = \text{PSL}(2, p)$ satisfies the replacement property, in some special cases, we can say if G has this property or not [4].

Theorem 32. *Let $G = \text{PSL}(2, p)$ and suppose that $m(G) = 4$. Then, G satisfies the replacement property.*

Proof. Let $s = (g_1, g_2, g_3, g_4)$ be an irredundant generating sequence of length 4 and let (M_1, M_2, M_3, M_4) be a corresponding sequence of maximal subgroups in general position. From Whiston and Saxl if $m = 4$, then at least two of the M_i must be isomorphic to S_4 or A_5 .

Let $\lambda(H)$ be the number of primes in the prime decomposition of $|H|$ (with multiplicities). For subgroups H_i in general position, $|H_i \cap H_j| < |H_i|$ for $i \neq j$ and so it must be that $\lambda(H_i \cap H_j) < \lambda(H_i)$. Since $|A_5| = 60 = 2^2 \times 3 \times 5$, $\lambda(A_5) = 4$. Similarly, $|S_4| = 24 = 2^3 \times 3$ and so $\lambda(S_4) = 4$ as well. If M_4 is isomorphic to S_4 or A_5 , then $\lambda(M_1 \cap M_4) \leq 3$, $\lambda(M_1 \cap M_2 \cap M_4) \leq 2$ and $\lambda(M_1 \cap M_2 \cap M_3 \cap M_4) \leq 1$. The aim is to show that this intersection is trivial, which is true if and only if $\lambda(\cap M_i) = 0$. Therefore, to find a contradiction, suppose that $\lambda(\cap M_i) = 1$. Then, $\lambda(M_1 \cap M_4) = 3$ and $\lambda(M_1 \cap M_2 \cap M_4) = 2$.

To begin, suppose that one of the $M_i \cong S_4$. Without loss of generality, suppose that $M_4 \cong S_4$. Then, consider the sequence $(M_1 \cap M_4, M_2 \cap M_4, M_3 \cap M_4)$ of subgroups in M_4 . The subgroups of S_4 are isomorphic to $A_4, D_8, S_3, \mathbb{Z}_2^2, \mathbb{Z}_4, \mathbb{Z}_3, \mathbb{Z}_2, \{e\}$. The only ones with $\lambda = 3$ are A_4 and D_8 . The intersection of any two of these will be a subgroup of A_4 or D_8 with $\lambda = 2$, of which there are only two: \mathbb{Z}_2^2 and \mathbb{Z}_4 .

Before proceeding, a quick fact is needed about $\mathbb{Z}_2^2 \leq S_4$. Let $V \leq D_8 \leq S_4$ be isomorphic to a subgroup \mathbb{Z}_2^2 . It is a standard exercise to show that for $G = S_4$, the derived subgroup $[G, G] = A_4$ and the second derived subgroup $[[G, G], [G, G]]$ isomorphic to V . The derived series are all normal subgroups (in G) and so V is normal in G . Since V sits inside a Sylow-2 subgroup (D_8) and all the Sylow-2 subgroups conjugate to each other, it must be that V sits inside each of the D_8 . The intersection of distinct D_8 must therefore be V since 4 is the largest proper divisor of 8. Therefore, the intersection between any two $M_i \cap M_4$ must be this V . Intersecting the two will again result in V and so the groups are not in general position. Therefore, all possible maximal subgroups intersect trivially and thus G satisfies the replacement property.

Next, suppose that one of the $M_i \cong A_5$. Without loss of generality, suppose that $M_4 \cong A_5$. Then, consider the sequence $(M_1 \cap M_4, M_2 \cap M_4, M_3 \cap M_4)$ of subgroups in M_4 . The subgroups of A_5 are isomorphic to $A_4, D_{10}, \mathbb{Z}_5, S_3, \mathbb{Z}_2^2, \mathbb{Z}_2, \{e\}$. The only one with $\lambda = 3$ is A_4 . The intersection of any two of these will be a subgroup of A_4 with $\lambda = 2$, of which there is only one: \mathbb{Z}_2^2 .

However, the claim is that two copies of A_4 in A_5 must intersect in a cyclic subgroup (including the trivial group). Suppose instead that there are two subgroups $H_1, H_2 \cong A_4$ that contain the same copy of V . It was already discussed that V is normal in H_1, H_2 (and as the Sylow-2 subgroup, is unique). Note that $H_1, H_2 \leq N_{A_5}(V)$. But, V cannot be normal in A_5 , because this is a simple group. On the other hand, A_4 is maximal. Therefore, $H_1 = H_2 = N_{A_5}(V) \cong A_4$. Thus, two distinct H_i cannot intersect in V and so G satisfies the replacement property. \square

The above proof is very specific to $G = \text{PSL}(2, p)$. One can give another proof which is more general and can be applied to other groups.

Theorem 33. (*R. K. Dennis, 2011*) *Let G be a finite group, $m = m(G)$ and $s = (g_1, \dots, g_m)$ is an irredundant generating sequence of length m . Let $F = \{M_1, \dots, M_m\}$ be an associated family of maximal subgroups in general position. Assume that for any such F , there exists one of the maximal subgroups, say M_m such that*

1. $M_m = \langle g_1, \dots, g_{m-1} \rangle$
2. $m(M_m) = m - 1$
3. M_m satisfies the replacement property.

Then, G satisfies the replacement property

Proof. Note that for $j \neq m$ we have

1. $M_m \cap M_j \geq \langle s(\hat{m}, \hat{j}) \rangle$ (the sequence generated by all the g_i for i not m and not j).
2. $M_m \cap M_j \neq M_m$ since F is in general position.
3. Thus, there exists $N_j \in \text{Max}(M_m)$ (the set of maximal subgroups of M_m) with $N_j \geq M_m \cap M_j$.
4. Hence, $F' = \{N_1, \dots, N_{m-1}\}$ is a family of maximal subgroups of M_m in general position associated to the irredundant generating sequence $s' = (g_1, \dots, g_{m-1})$.
5. Since M_m satisfies the replacement property, we have that $N_1 \cap \dots \cap N_{m-1}$ is trivial.
6. Thus, $M_1 \cap \dots \cap M_m = (M_m \cap M_1) \cap \dots \cap (M_m \cap M_{m-1}) \leq N_1 \cap \dots \cap N_{m-1} = \{e\}$. Therefore, G satisfies the replacement property.

□

This generalization can then be applied to $\text{PSL}(2, p)$ and at least also the sporadic group M_{11} :

Corollary 34. *Let $G = \text{PSL}(2, p)$, p prime and $m(G) = 4$. Then, G satisfies the replacement property.*

Proof. We know that every F must contain a group isomorphic to either S_4 or A_5 . Call this subgroup H . Furthermore, H is strongly flat, i.e. for $K < H$, $m(K) < m(H)$. That is, the only irredundant sets of length 4 in H are generating sets for H . Let s be an irredundant generating set of length 4 for G . Since both S_4 and A_5 satisfy the replacement property, by the theorem, so does G . □

Corollary 35. *(R. K. Dennis, 2011) $G = M_{11}$ satisfies the replacement property*

Proof. A combination of computations and simple arguments show that $m(G) = 5$. Furthermore, it is a fact that $H = \text{PSL}(2, p)$ is always one of the maximal subgroups in an F . We know that $m(H) = 4$ and every subgroup of H has m at most 3. Furthermore, we have just proved that H satisfies the replacement property. Thus, by the theorem, G satisfies the replacement property. □

However, $\text{PSL}(2, p)$ does not satisfy the replacement property in general:

Theorem 36. *Let p be a prime with $p \equiv +1 \pmod{8}$. Let $G = \text{PSL}(2, p)$. If $m(G) = 3$, then G fails the replacement property.*

Proof. In order to show that G fails the replacement property, this proof produces an explicit example of an element $w \in G$ and a length three generating set $\{g_1, g_2, g_3\}$ such that replacing any g_i by w will result in a set which no longer generates G . Since it is easier to work with matrices than with elements in $\text{PSL}(2, p)$, often, elements in $\text{SL}(2, p)$ will be used instead of their projections into G . For the sake of clarity, capital letters will denote elements in $\text{SL}(2, p)$ and lower case letters will denote their projections in $G = \text{PSL}(2, p)$.

Consider four elements in G , denoted a, b, c, w . If $\pi : \text{SL}(2, p) \rightarrow G$, is the canonical projection, then let A, B, C, W be such that $\pi(A) = a, \pi(B) =$

$b, \pi(C) = c$ and $\pi(W) = w$. We will construct a, b, c, w such that $\{wa, wb, wc\}$ is a length 3 irredundant generating set of G , but the element w will be such that it cannot replace any of these elements to recover a generating sequence. For $r, s, t, u \in \mathbb{F}_p$ let

$$A = \begin{pmatrix} r & s \\ s & -r \end{pmatrix} \quad B = \begin{pmatrix} t & u \\ u & -t \end{pmatrix} \quad W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \quad (1)$$

Since A and B have determinant 1, $r^2 + s^2 = t^2 + u^2 = -1$. Note that A, B and W are traceless. By Lemma 50, it must be that A, B and W have order 4 and a, b and w have order 2. Furthermore, notice that

$$WA = \begin{pmatrix} -s & r \\ r & s \end{pmatrix} \quad WB = \begin{pmatrix} -u & t \\ t & u \end{pmatrix} \quad AW = \begin{pmatrix} s & -r \\ -r & -s \end{pmatrix} \quad BW = \begin{pmatrix} u & -t \\ -t & -u \end{pmatrix}, \quad (2)$$

and so $AW = -WA$ and similarly, $BW = -WB$. Since AW, AB are still traceless, aw and bw also have order 2. Therefore, $\langle a, w \rangle = \{a, w, aw, \text{id}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and likewise, $\langle b, w \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Now, generically write

$$C = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad (3)$$

where $\alpha\delta - \beta\gamma = 1$. Examples have shown that c can be chosen to have order 2, so let $\alpha + \delta = 0$. Furthermore, $\text{Tr}(WC) = +1$ which by Lemma 50 means that the order of wc is 3. The product WC has the form

$$WC = \begin{pmatrix} -\gamma & -\delta \\ \alpha & \beta \end{pmatrix}, \quad (4)$$

and so the condition that $\text{Tr}(WC) = +1$ becomes $\beta - \gamma = +1$. In the data, it appears that one can make the choice $\beta = 0$ so that $\gamma = -1$. Furthermore since $\alpha\delta - \beta\gamma = 1$, $\beta = 0$ implies that $\alpha = \delta^{-1}$ and since the trace of C is zero, $\alpha = -\delta$. Thus, $\alpha^{-1} = -\alpha$, or α has order 4 in \mathbb{F}_p . Does such an element exist? Since $p \equiv 1 \pmod{8}$, $8|(p-1)$, which is the order of the cyclic group \mathbb{F}_p^* . Therefore, \mathbb{F}_p^* has an element of order 8 and so also has an element of order 4. Fix such an element and call it i . Then,

$$C = \begin{pmatrix} -i & 0 \\ -1 & i \end{pmatrix}. \quad (5)$$

Note that

$$w(cw)w^{-1} = wcww = wc. \quad (6)$$

However, since $(cw)(wc) = 1$,

$$w(cw)w^{-1} = (cw)^{-1}. \quad (7)$$

Therefore, $\langle c, w \rangle = \langle w, wc \rangle = \langle x, y | x^2 = y^3 = 1, xyx^{-1} = y^{-1} \rangle \cong S_3$. The last isomorphism in the preceding sentence is due to a standard presentation of S_3 , for example given in Section 1.2 of [7]. The next step is to show that $\langle aw, cw \rangle \cong S_4$. The idea is to use the trace technology laid out in Theorem 51. In order to apply the theorem, some nonzero traces are required. The trace of WA is 0 and the trace of $WC = +1$. Therefore, the Theorem 51 only applies if $WCWA$ has a particular trace. Multiplying these elements gives rise to the following matrix:

$$WCWA = \begin{pmatrix} -s - ir & r - is \\ is & -ir \end{pmatrix}, \quad (8)$$

so that $\text{tr}(WCWA) = -s - 2ir$. The required constraint from the Theorem is that $(s + 2ir)^2 = 2$. If this holds, then Theorem 51 says that $\langle aw, cw \rangle \cong S_4$ if $\text{tr}([WA, WC]) = +1$. Simple arithmetic using the forms of A, C and W yields the following computation:

$$\begin{aligned} \text{tr}([WA, WC]) &= \text{tr}[(WA)(WC)(WA)^{-1}(WC)^{-1}] \\ &= \text{tr}[WAWCAWCW] \\ &= -\text{tr}[(AWC)^2] \\ &= -2i^2s^2 + 4isr - r^2 + 2i^2r^2 \\ &= 2s^2 + 4isr - 3r^2. \end{aligned} \quad (9)$$

Setting this expression equal to 1 and using the constraint that $s^2 + r^2 = -1$ (from the determinant), one finds that

$$3s^2 + 4isr - 2r^2 = 0, \quad (10)$$

which has solution

$$r = \left(i \pm \frac{\sqrt{2}}{2} \right) s, \quad (11)$$

and then inserting this back into $s^2 + r^2 = -1$, one arrives at

$$s^2 = -\frac{2}{9} \pm \frac{4}{9}i\sqrt{2} = \left[\frac{1}{3} \left(2i \pm \sqrt{2} \right) \right]^2, \quad (12)$$

and so the question has simply boiled down to the existence of an element $\zeta \in \mathbb{F}_p$ such that $\zeta^2 = 2$ (and $p \neq 3$, so 3^{-1} makes sense). It is a standard result in elementary number theory (c.f. [12]) that 2 has a square root if $p \equiv \pm 1 \pmod{8}$ (fix one and call it $\sqrt{2}$). Therefore, all that is left to show in order to apply Theorem 51 is for $\text{tr}(WCWA) = -s - 2ir$ to have the correct form. Using the expressions for r and s above, a quick computation shows that $-s - 2ir = \sqrt{2}$, as required by the theorem. Therefore, $\langle wa, wc \rangle \cong S_4$. An analogous discussion shows that if one fixes s as one solution to Eq. 12, then picking the other solution for u and constructing t as was done for r will give $\langle wb, wc \rangle \cong S_4$ as well.

The strategy to demonstrate that w cannot replace wa, wb or wc will be to show that w is in the subgroups generated by (maximal subgroups containing) $\langle wa, wc \rangle$, $\langle wb, wc \rangle$ and $\langle wa, wb \rangle$. The first step in this process is to prove that $\langle wa, wc \rangle = \langle a, c, w \rangle$. Note that

$$WAWC = -AWWC = AC, \quad (13)$$

and since $(ac)(ca) = 1$, $ac, ca \in \langle wa, wc \rangle$. Furthermore, since $(wc)(cw) = (aw)(wa) = 1$, $cw, wc, aw, wa \in \langle wa, wc \rangle$. Now, take any element $x \in$

$\langle a, c, w \rangle$. By construction, such an element can be written as a string in the alphabet $a, c, w, a^{-1} = a, c^{-1} = c, w^{-1} = w$ (no need to worry about uniqueness). Suppose that x can be written with an even number of letters in the string. Then, this element is in $\langle wa, wc \rangle$ because every possible pairing of letters from the above alphabet is in $\langle wa, wc \rangle$. For example, consider the word

$$x = awcwaccwawcw. \quad (14)$$

One can group these letters into pairs:

$$x = (aw)(cw)(ac)(cw)(aw)(cw). \quad (15)$$

and then it is clear that every element in parenthesis is in $\langle wa, wc \rangle$. Instead of an even number of letters, suppose that x can be written as a string with an odd number of letters from the alphabet. Then, one can form x from a string in $\langle wa, wc \rangle$ by adding one of a, b, w . This is clear because if there are n letters that make up x , then $n - 1$ will be an even number and so the substring of the first $n - 1$ letters will be in $\langle wa, wc \rangle$ by the preceding argument. Thus, every element in $\langle a, c, w \rangle$ can be formed from an element in $\langle wa, wc \rangle$ by adding one of a, c, w or id . This means that

$$|\langle a, c, w \rangle| \leq 4|\langle wa, wc \rangle|. \quad (16)$$

However, from above, $\langle wa, wc \rangle \cong S_4$ so $|\langle a, c, w \rangle| \leq 96$. Furthermore, by Dickson's Theorem, S_4 is maximal in G and so no proper subgroup can contain $\langle wa, wc \rangle$. Therefore, either $\langle a, c, w \rangle = \langle wa, wc \rangle$ or $\langle a, c, w \rangle = G$. Since $p \equiv 1 \pmod{8}$, $p \geq 17$ so $|G| \geq 2448 > 96$ and thus $\langle a, c, w \rangle = \langle wa, wc \rangle$. By an analogous argument, $\langle b, c, w \rangle = \langle wb, wc \rangle$. The last consideration is to study $\langle wa, wb \rangle$. This group is generated by two elements of order 2 and so must be dihedral. To see how large it is, one needs to know the order of $wawb = awwb = ab$. This amounts to computing the trace of AB , which is

$$\text{tr}(AB) = 2(rt + su) = -8i/3. \quad (17)$$

This is certainly not zero and a quick arithmetic computation shows that it is also not ± 1 or $\pm\sqrt{2}$. Therefore, by Lemma 50, the order of ab is more

than 4 and so $ab \notin S_4$. It is also clear that $\langle wa, wb \rangle \neq G$ because G is not dihedral. The final step before concluding is to show that $\langle a, b, w \rangle$ is a proper subgroup of G . This procedure is similar to the one above by considering the index of $\langle wa, wb \rangle$ in $\langle a, b, w \rangle$. Since $wawb = ab \in \langle wa, wb \rangle$, as before, every possible pair of letters in $\langle a, b, w \rangle$ is in $\langle wa, wb \rangle$ and therefore, one arrives at the same bound as earlier:

$$|\langle a, b, w \rangle| \leq 4|\langle wa, wb \rangle|. \quad (18)$$

Recall that $\langle wa, wb \rangle$ is dihedral. From Dickson's Theorem, the largest dihedral subgroup of G has order $p + 1$. Therefore

$$|\langle a, b, w \rangle| \leq 4|\langle wa, wb \rangle| \leq 4(p + 1) < p(p + 1)(p - 1)/2. \quad (19)$$

Since for $p \geq 17$, $p(p - 1)/2 = 136$. Let M be a maximal subgroup of G which contains $\langle wa, wb \rangle$. Since $\langle a, b, w \rangle$ is proper and contains $\langle wa, wb \rangle$, $w \in M$.

Now, all the machinery is in place to conclude. The set $\{wa, wb, wc\}$ will generate G because $wb \notin \langle wa, wc \rangle$ and $\langle wa, wc \rangle$ is maximal, so the subgroup generated by all three elements, which contains a maximal subgroup, must be all of G . Furthermore, it is clear that w cannot replace any of wa, wb, wc because w is in the maximal subgroup containing each pair. Explicitly, the set $\{w, wb, wc\}$ cannot generate G because $w \in \langle wb, wc \rangle \cong S_4$. The same holds for replacing wb . Finally, w cannot replace wc because the maximal subgroup which contains $\langle wa, wb \rangle$ also contains w and so $\langle w, wa, wb \rangle \leq M < G$. Therefore G fails the replacement property if $m(G) = 3$. \square

Corollary 37. *If $p \not\equiv \pm 1 \pmod{10}$ and $p \neq 7$ but $p \equiv +1 \pmod{8}$, then G fails the replacement property.*

Question 38. What are all the cases for which G satisfies the replacement property when $m(G) = 3$?

5. Elements of Irredundant Generating Sequences, ι

Define $\iota_n(G)$ to be the set of orders of elements which appear in length n generating sequences. Clearly, for $n > m(G)$, $\iota_n(G)$ is the empty set. For

$G = \text{PSL}(2, p)$, $\iota_1(G)$ is also the empty set, since G is not cyclic. Robert Guralnick [10] has proved a powerful theorem about length two generating sets of simple groups³:

Theorem 39 (3/2 Generation). *Given any $x \in G$, there exists a $y \in G$ so that $G = \langle x, y \rangle$. In particular, $r(G) = 2$ for any G a non-abelian finite simple group.*

Therefore, by the 3/2 Generation Theorem, $\iota_2(G) = \{d \mid d \text{ divides } |G| \text{ and } d \text{ is not } 1\}$ (every non-identity element is in a length 2 [irredundant] generating sequence). Thus, all that remains to be determined is $\iota_3(G)$ and $\iota_4(G)$. For solvable groups, all the elements of a generating sequence of maximal length have prime order [4]. For simple groups, this is not necessarily true. We can see this as a result of the following proposition:

Proposition 40. *For $G = \text{PSL}(2, p)$, there is always a length 3 irredundant generating sequence where all three elements have order $(p - 1)/2$.*

Proof. Let $\pi : \text{SL}(2, p) \rightarrow G$ be the canonical projection. Let a, b, c be elements of G and A, B, C be lifts to matrices in $\text{SL}(2, p)$. Define:

$$A = \begin{pmatrix} x & 0 \\ 0 & \frac{1}{x} \end{pmatrix} \quad B = \begin{pmatrix} \frac{1}{x} & 0 \\ x & x \end{pmatrix} \quad C = \begin{pmatrix} \frac{1}{x} & y \\ 0 & x \end{pmatrix}, \quad (20)$$

where $x \in \mathbb{F}_p^*$ and

$$y = -x + \frac{2}{x} - \frac{1}{x^3}. \quad (21)$$

Note that A, B and C have order $p - 1$ and so a, b and c have order $(p - 1)/2$. We claim that a, b, c is the sequence we seek. First, we note that

$$AB = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad (22)$$

which is the ‘canonical’ element of order p . Furthermore,

³This proof invokes the classification of finite simple groups.

$$AC = \begin{pmatrix} 1 & xy \\ 0 & 1 \end{pmatrix} \quad BC = \begin{pmatrix} \frac{1}{x^2} & \frac{y}{x} \\ 1 & xy + x^2 \end{pmatrix}, \quad (23)$$

which both have trace 2 and thus have order p . It is clear that A is not in $\langle B \rangle \cup \langle C \rangle$, B is not in $\langle A \rangle \cup \langle C \rangle$ and C is not in $\langle A \rangle \cup \langle B \rangle$, since A is diagonal, B is upper triangular and C is lower triangular. Furthermore, it is clear that $\langle a, b \rangle$, $\langle a, c \rangle$ are not all of G because there will always be a zero in the upper right (lower left) position. Since each of these groups contain an element of order p and one of order $(p-1)/2$, they are contained in an H_i and thus must exactly generate the H_i . All that remains to show is that $\langle b, c \rangle$ is not all of G . To do this, we will observe that $\langle bc \rangle \trianglelefteq \langle b, c \rangle$. This will give us the desired result, since G is simple and so has no normal subgroups (and bc has order p , so is a proper nontrivial subgroup). First, a simple computation shows that

$$(BC)^n = \begin{pmatrix} \frac{n-(n-1)x^2}{x^2} & \frac{-n(-2x^2+1+x^4)}{x^4} \\ n & \frac{-n+(n+1)x^2}{x^2} \end{pmatrix}. \quad (24)$$

In order to show that BC is normal, we need to show that conjugating by B, B^{-1}, C, C^{-1} takes BC to another power of BC . A simple computation shows that

$$(BC)^{x^2} = CB, \quad (25)$$

which means that $CB = C(BC)C^{-1} \in \langle BC \rangle$ and similarly $CB = B^{-1}(BC)B \in \langle BC \rangle$. Finally, note that

$$(BC)^{x^{-2}} = B(CB)B^{-1} = C^{-1}(BC)C. \quad (26)$$

Therefore, $\langle BC \rangle$ is normal in $\langle B, C \rangle$ since any power of BC conjugates to another power of BC by the generators of $\langle B, C \rangle$, for example

$$B(BC^n)B^{-1} = B(BC)B^{-1}B(BC)B^{-1} \cdots B(BC)B^{-1} \in \langle BC \rangle. \quad (27)$$

□

Corollary 41. *Let G be a group. The elements of maximal length irredundant generating sequences of G need not have prime order if G is not solvable.*

Proof. We know that for $G = \text{PSL}(2, 13)$, $m(G) = 3$. Furthermore, by the lemma, there exists an irredundant generating sequence of length 3 such that all the elements have order 6. \square

Corollary 42. *Every divisor of $(p - 1)/2$ is in $\iota_3(G)$.*

Proof. Let g_1, g_2, g_3 be a length three irredundant generating set as in the lemma. Take any $x \in \langle g_1 \rangle$ (i.e. an element whose order divides the order of g_1 , which is $(p - 1)/2$). Since the intersection of all the subgroups $\langle g_i, g_j \rangle$ is trivial, this sequence satisfies the replacement property by Cor 8. Therefore, x can replace one of the g_i to arrive at a new generating sequence. Clearly, it can only replace g_1 . This new generating set x, g_2, g_3 is still irredundant because the set of maximal subgroups in general position associated to the set is the same as it was for the original set of the g_i . \square

Now, let's consider the elements whose order divide $p + 1$ or have order p . To proceed, we will need the following lemma:

Lemma 43. *Let $x \in G = \text{PSL}(2, p)$, $p > 5$. If x has order p or order > 5 dividing $p + 1$, then there is a unique maximal subgroup of G which contains x .*

Proof. First, we note that a dihedral group D of order $2n = p + 1$ has a unique cyclic subgroup of order q for every $q > 2$ which divides n . This subgroup will be contained in the index two cyclic subgroup of D which is characteristic. Therefore, the cyclic subgroup Q of order q is normal in D . Since G is simple, $N_G(Q) \neq G$. Suppose that Q is contained in some maximal subgroup M containing $N_G(Q)$. Note that $N_D(Q) = D$ since Q is normal in D . Therefore, $D \leq N_G(D)$, but D is maximal in G , so $N_G(D) = D$, i.e. $M = D$; there is a unique maximal subgroup of G which contains Q , namely $N_G(Q)$.

Now, suppose that x has order p . Since $p > 5$, the only maximal subgroup which can contain $\langle x \rangle$ is one isomorphic to $\mathbb{Z} \rtimes \mathbb{Z}_{(p-1)/2}$. However, $\langle x \rangle$ is normal in such a subgroup. Therefore, the same argument as above applies; there is a unique maximal subgroup which contains $\langle x \rangle$. \square

Corollary 44. *If $x \in \text{PSL}(2, p)$ has order > 5 that divides $p+1$ or has order p , then x is not in a length 3 irredundant generating sequence.*

Proof. Suppose that $\langle g_1, g_2, g_3 \rangle$ is an irredundant generating sequence of length 3 and suppose that g_1 has order which divides $p+1$ or has order p . Then, there is a unique maximal subgroup which contains g_1 . Let M_1, M_2, M_3 be the associated set of maximal subgroups in general position. Since there is a unique maximal subgroup which contains g_1 , $M_2 = M_3$, which contradicts the fact that they are in general position. Thus, the sequence of the g_i cannot be irredundant. \square

Now, we are ready to list what we know about $\iota_n(G)$:

Theorem 45. *Let $G = \text{PSL}(2, p)$. Then, for $n > 4$, $\iota_1(G) = \iota_n(G) = \{\}$. In addition, $\iota_2(G) = \{d \mid d \text{ divides } |G| \text{ and } d \text{ is not } 1\}$. Then, there are several cases for ι_3 and ι_4 :*

$$\iota_3(G)$$

$\{d \mid d \text{ divides } p-1\} \leq \iota_3(G)$. This is all of $\iota_3(G)$ unless one of the following is true.

1. $p \equiv -1 \pmod{10}$. Then, 5 may also be in $\iota_3(G)$.
2. $p \equiv -1 \pmod{8}$. Then, 4 may also be in $\iota_3(G)$.
3. $p \equiv -1 \pmod{3}$ and $(p \equiv 3, 13, 27, 37 \pmod{40}, p \equiv \pm 1 \pmod{8} \text{ or } p \equiv \pm 1 \pmod{10})$. Then, 3 may also be in $\iota_3(G)$.

$$\iota_4(G)$$

1. $p \not\equiv \pm 1 \pmod{8}$ and $p \not\equiv \pm 1 \pmod{10}$. Then $\iota_4(G) = \{\}$.
2. $p \not\equiv \pm 1 \pmod{8}$. Then, $\iota_4(G) = \{2\}$ if $p = 7$ and $\iota_4(G) = \{\}$ otherwise.
3. $p \equiv \pm 1 \pmod{10}$. Then, $\iota_4(G) \subseteq \{2, 3\}$.

Proof. $\iota_1(G)$ is empty because G is not cyclic. $\iota_n(G)$ for $n > 4$ is empty because Whiston and Saxl showed that $m(G) \leq 4$.

Now, let's consider $\iota_3(G)$. By Cor. 42, every divisor of $(p-1)/2$ is in $\iota_3(G)$. To get that 2 is in $\iota_3(G)$, we have to do some additional work. Let H

be the subgroup generated by all the elements of order 2. Such a subgroup is normal and since G is simple, it must be all of G . Also, since G is not dihedral, it must be that no length two sequence of elements of H generates G . If $m(G) = 3$, then we immediately get that there exists a length three irredundant generating sequence of length 3. If $m(G) = 4$, then it is possible that there is a length four irredundant generating sequence such that the order of each element is 2. Then, one must apply a further argument [4] to show that there also exist length 3 irredundant generating sequences with elements of order 2. Cor. 44 says that every divisor of $p + 1$ that is greater than 5 is not in an irredundant length 3 generating sequence. The corollary extends if no other [exceptional] maximal subgroups which can contain elements of orders which divide $p + 1$. Case 1 is when 5 divides $p + 1$ and the exceptional subgroups A_5 exists which could contain elements of order 5. Likewise, Case 2 is when S_4 is a maximal subgroup and 4 divides $p + 1$. The third case covers the possibility that elements of order 3 divide $p + 1$ and also could be contained in an exceptional maximal subgroup of type A_5, A_4 or S_4 . For example, if $p = 11$, then $3|(p + 1)$ but there exists a length 3 irredundant generating sequence such that each element has order 3 and each pair generates an isomorphic copy of A_5 .

Finally, we will consider $\iota_4(G)$. We know that when G does not contain S_4 or A_5 as a maximal subgroup, then $m(G) = 3$ and so $\iota_4(G) = \emptyset$. If $p \equiv \pm 1 \pmod{8}$ then we know that $m(G) = 3$ unless $p = 7$, in which case all length 4 irredundant generating sequences have elements of order 2. Finally, for $p \equiv \pm 1 \pmod{10}$, we know that elements in length 4 irredundant generating sequences can have orders 2 or 3 only. \square

Question 46. What is $\iota_3(G) \cap \{3, 4, 5\}$ in general?

6. $m(G)$ when $p \equiv \pm 1 \pmod{10}$

The strategy presented here for $p \not\equiv \pm 1 \pmod{10}$ does not readily generalize because element orders are not restricted to be just 2. However, we can make restrictions on the length four generating sequences for $p \equiv \pm 1 \pmod{10}$. As before, let g_1, g_2, g_3, g_4 be a length four irredundant generating sequence of $G = \text{PSL}(2, p)$ and H_i the corresponding set of subgroups in general position. Furthermore, let $H_i \leq M_i$ be a set of maximal subgroups in general position. From lemmas that we have proven already, we know that

all the g_i have order 2 or 3. In addition, without loss of generality, $H_1 \cong M_1$ is isomorphic to S_4 or A_5 and likewise $H_2 \cong M_2$ is also isomorphic to either of these exceptional groups. The remaining M_3 and M_4 can be either dihedral or one of these two exceptional types. If they are both dihedral, then we can even note that they must be of the same type:

Lemma 47. *If M_3 and M_4 are dihedral, then $M_3 \cong M_4$.*

Proof. Without loss of generality, suppose that $M_3 \cong D_{p+1}$ and $M_4 \cong D_{p-1}$. Then, $M_3 \cap M_4$ must have order which is a divisor of both $p+1$ and $p-1$. However, $(p+1, p-1) = 2$ and so the intersection is either trivial or cyclic of order 2. This is impossible if the M_i are to be in general position. \square

We can also extend Cor. 19 to cases there there is an A_5 :

Lemma 48. *Suppose that all the g_i have order 2. No two of $\text{Order}(g_1g_2)$, $\text{Order}(g_1g_3)$ and $\text{Order}(g_2g_3)$ can be 3, no two can be 4 and no two can be 5.*

We have carried out computations using the above lemmas to place further restrictions on the available groups. However, there are many cases in which the Todd-Coxeter approach does not terminate in a reasonable amount of time. It may turn out that additional lemmas can pinpoint the answer to the following question, whose answer would complete our understanding of $m(G)$ for all primes.

Question 49. Are there more than 3 cases of $m = 4$ when $p \equiv \pm 1 \pmod{10}$?

Answering this question may also require discovering new methods. For example, the proof may be achievable with a variation on Hall's 1936 paper [11] which gives the lattice of subgroups, Moebius function and a formula for $\phi_n(G)$. We will now end with some computations involving the four known cases where $m(G) = 4$.

7. Computations involving the four known cases.

For a description of the computations, see [14]. Examples of length four irredundant generating sequences (lifted to $\text{SL}(2, p)$ so one can see the matrices) are below for (respectively) $p = 7, 11, 19, 31$:

$$\left\{ \begin{pmatrix} 4 & 6 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 5 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 6 \\ 1 & 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 & 5 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 8 & 10 \end{pmatrix}, \begin{pmatrix} 4 & 8 \\ 2 & 7 \end{pmatrix} \right\}$$

$$\left\{ \begin{pmatrix} 4 & 7 \\ 3 & 15 \end{pmatrix}, \begin{pmatrix} 1 & 18 \\ 2 & 18 \end{pmatrix}, \begin{pmatrix} 18 & 14 \\ 8 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 8 \\ 16 & 17 \end{pmatrix} \right\}$$

$$\left\{ \begin{pmatrix} 3 & 30 \\ 10 & 28 \end{pmatrix}, \begin{pmatrix} 25 & 27 \\ 17 & 6 \end{pmatrix}, \begin{pmatrix} 17 & 1 \\ 20 & 14 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 23 & 30 \end{pmatrix} \right\}$$

Note that all of these elements have zero trace and so each have order 2. We summarize properties of the possible sequences in Tables 7 and 11. The fact that for $p = 31$ there is only one automorphism class of length 4 irredundant generating sequences was already known to P. Cara (see the announcement [3]).

	$p = 7$	$p = 11$
Length 4 irredundant generating sets	252	11935
Conjugacy classes of sets	2	22
Automorphism classes of sets	2	14
Possible Orders of Elements	2	2,3
Families of Maximal Subgroups	S_4, S_4, S_4, S_4	A_5, A_5, A_5, A_5 A_5, A_5, A_5, D_{12} A_5, A_5, D_{12}, D_{12}

Table 10: Properties of length four generating sequences for $p = 7$ and $p = 11$.

	$p = 19$	$p = 31$
Length 4 irredundant generating sets	7695	14880
Conjugacy classes of sets	4	1
Automorphism classes of sets	3	1
Possible Orders of Elements	2	2
Families of Maximal Subgroups	A_5, A_5, A_5, A_5 A_5, A_5, A_5, D_{20} A_5, A_5, D_{20}, D_{20}	S_4, S_4, A_5, A_5

Table 11: Properties of length four generating sequences for $p = 19$ and $p = 31$.

8. Acknowledgements

This work would not have been possible without countless discussions with K. Dennis. In particular, Lemmas 11, 26, 43, 47 and Corr. 44 were directly discovered during such discussions and others were the byproduct of these conversations. The author is grateful for K. Dennis' encouragement and academic support.

Appendix A. Some properties of traces in $\text{PSL}(2, p)$

The following properties of traces are from [13] and [15].

Lemma 50. *Let I be the 2×2 identity matrix and take $\pm I \neq x \in \text{SL}(2, \mathbb{F})$. Then,*

1. $x^2 \neq I$ if and only if $p = 2$ and $\text{tr}(x) = 0$.
2. $x^2 = -I$ if and only if $\text{tr}(x) = 0$.
3. $x^3 = \pm I$ if and only if $\text{tr}(x) = \mp 1$.
4. $x^4 = -I$ if and only if $\text{tr}(x) = \pm\sqrt{2}$.

One can use trace identities to write down conditions for other orders as well [9]. For example, for $A \in \text{SL}(2, p)$, $A \neq \pm I$ and $\pm \text{tr}(A)^3 + \text{tr}(A)^2 \mp 2\text{tr}(A) - 1 = 0$ then A has order 7. Similarly, if $\text{tr}(A)^2 \pm \text{tr}(A) - 1 = 0$ then A has order 5.

In fact, the traces of elements even carry information about subgroups. For example, there is a theorem by McCullough [13] which relates traces of elements to the subgroup that they generate. One result from this theorem was used in Theorem 36. The unpublished paper [13] considers a slightly different case than the present one, but the proof goes through without much modification. Let $p \equiv 1 \pmod{8}$ (so that $\sqrt{2} \in \mathbb{F}_p$ - see for example [12]). The following is true [13]:

Theorem 51. *Let $A, B \in \text{SL}(2, p)$ with no more than one of $\text{tr}(A), \text{tr}(B), \text{tr}(AB)$ equal to zero. Then, $\pi(\langle A, B \rangle) = S_4$ if $\text{tr}(A), \text{tr}(B), \text{tr}(AB) \in \{0, \pm 1, \pm\sqrt{2}\}$ (and at least one is $\pm\sqrt{2}$) and $\text{tr}([A, B]) = 1$.*

Before proving this, preliminary lemmas need to be established to build some trace technology in $\text{SL}(2, p)$.

Lemma 52. *Let $a, b \in \text{SL}(2, \mathfrak{p})$. Let $\pi : \text{SL}(2, \mathfrak{p}) \rightarrow \text{PSL}(2, \mathfrak{p})$ be the standard projection. Then, $\pi(\langle a, b \rangle)$ is the same as each of the following groups:*

$$\pi(\langle a^{-1}, b \rangle), \pi(\langle b, a \rangle), \pi(\langle a^{-1}, ab \rangle), \pi(\langle -a, b \rangle), \pi(\langle -a, -b \rangle)$$

.

Proof. This is clear since $\pi(a) = \pi(-a)$. \square

Now, the goal is to see how these actions on the set of generators change the traces of the generators. Then, one can simply look at traces of elements instead of the elements themselves. To attack this, it is necessary to establish a few trace identities in $\text{SL}(2, \mathfrak{p})$.

Lemma 53. *For $a, b \in \text{SL}(2, \mathfrak{p})$, $\text{tr}(a^{-1}b) + \text{tr}(ab) = \text{tr}(a)\text{tr}(b)$.*

Proof. Take

$$a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad b = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad (\text{A.1})$$

Then,

$$a^{-1}b = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{22}b_{11} - a_{12}b_{21} & a_{22}b_{12} - a_{12}b_{22} \\ -a_{21}b_{11} + a_{11}b_{21} & -a_{21}b_{12} + a_{11}b_{22} \end{pmatrix} \quad (\text{A.2})$$

$$ab = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}, \quad (\text{A.3})$$

therefore,

$$\begin{aligned} \text{tr}(a^{-1}b) + \text{tr}(ab) &= a_{11}b_{11} + a_{12}b_{21} + a_{21}b_{12} + a_{22}b_{22} - a_{22}b_{11} + a_{12}b_{21} + a_{21}b_{12} - a_{11}b_{22} \\ &= a_{22}b_{11} + a_{11}b_{22} + a_{11}b_{11} + a_{22}b_{22} \\ &= (a_{11} + a_{22})(b_{11} + b_{22}) \\ &= \text{tr}(a)\text{tr}(b). \end{aligned} \quad (\text{A.4})$$

\square

Lemma 54 (Fricke). *For $a, b \in SL(2, p)$, $\text{tr}([a, b]) = \text{tr}(a)^2 + \text{tr}(b)^2 + \text{tr}(ab) - \text{tr}(a)\text{tr}(b)\text{tr}(ab) - 2$*

Proof. All that is required is the repeated use of the previous lemma and its immediate consequences such as $\text{tr}(a^2) = \text{tr}(a)^2 - 2$. The first computation is

$$\begin{aligned} \text{tr}(a)\text{tr}(b)\text{tr}(ab) &= \text{tr}(a) [\text{tr}(b^{-1}ab) + \text{tr}(ab^2)] \\ &= \text{tr}(a)^2 + \text{tr}(a)\text{tr}(ab^2) \\ &= \text{tr}(a)^2 + \text{tr}(b^2) + \text{tr}(a^2b^2) \\ &= \text{tr}(a)^2 + \text{tr}(b)^2 - 2 + \text{tr}(a^2b^2), \end{aligned} \tag{A.5}$$

which means that the righthand side of the lemma is $\text{tr}(ab)^2 - \text{tr}(a^2b^2)$. The next computation is the lefthand side:

$$\begin{aligned} \text{tr}(aba^{-1}b^{-1}) &= \text{tr}(a^{-1}b^{-1}ab) = \text{tr}((ba)^{-1}(ab)) = \text{tr}((ba)^{-1})\text{tr}(ab) - \text{tr}(baab) \\ &= \text{tr}(ab)^2 - \text{tr}(a^2b^2). \end{aligned} \tag{A.6}$$

and so the Fricke trace identity is proved. □

Now, it is possible to return to considering the consequences of Lemma 52. Let $T(a, b) = (\text{tr}(a), \text{tr}(b), \text{tr}(ab))$. For each of the equivalent generating sets in Lemma 52, the goal is to write down the sets of equivalent traces.

Lemma 55. *Let $a, b \in SL(2, p)$. Let $\pi : SL(2, p) \rightarrow PSL(2, p)$ be the standard projection. Then, one can always pick a different generating set a', b' of $\pi(\langle a, b \rangle)$ so that if $T(a, b) = (\alpha, \beta, \gamma)$ then $T(a', b')$ can be chosen to be one of the following:*

$$(\alpha, \beta, \alpha\beta - \gamma), (\beta, \alpha, \gamma), (\alpha, \gamma, \beta), (-\alpha, \beta, -\gamma), (-\alpha, -\beta, \gamma).$$

Proof. First, note that one can choose (a^{-1}, b) as a generating set. Since $\text{tr}(a^{-1}) = \alpha$, all that needs to be computed is

$$\mathrm{tr}(a^{-1}b) = \mathrm{tr}(a)\mathrm{tr}(b) - \mathrm{tr}(ab) = \alpha\beta - \gamma. \quad (\text{A.7})$$

Next, note that (b, a) can be used as a generating set. Trivially, this leaves the trace of the product unchanged and simply swaps α and β . Now, consider (a^{-1}, ab) as a generating set. This switches β and γ , leaving α unchanged. The multiplication by the negative signs is trivial; clearly if $(-a, b)$ is used as a generating set, the traces will be $(-\alpha, \beta, -\gamma)$ and if both a and b are negated, there is no change to the trace of the product. \square

Now, Theorem 51 can be proved.

Theorem 51. First of all, by the lemma, if B has trace $\sqrt{2}$, then A and B can be switched and generate the same group. Similarly, if AB has trace $\sqrt{2}$, then one can switch A and AB and generate the same group. Therefore, without loss of generality, suppose that $\mathrm{tr}(A) = \sqrt{2}$. Since no two of $\mathrm{tr}(A), \mathrm{tr}(B), \mathrm{tr}(AB)$ are zero, by the same logic one can take $\mathrm{tr}(B)$ to be nonzero. Let $\mathrm{tr}(A) = \alpha$, $\mathrm{tr}(B) = \beta$ and $\mathrm{tr}(AB) = \gamma$. First, consider the case where $(\alpha, \beta) = (\sqrt{2}, \sqrt{2})$. By the Fricke trace identity

$$\mathrm{tr}([A, B]) = \mathrm{tr}(A)^2 + \mathrm{tr}(B)^2 + \mathrm{tr}(AB) - \mathrm{tr}(A)\mathrm{tr}(B)\mathrm{tr}(AB) - 2 \quad (\text{A.8})$$

for $\gamma \in \{-\sqrt{2}, -1, 0, 1, \sqrt{2}\}$, the possible values of $\mathrm{tr}([A, B])$ are respectively $(4 + 2\sqrt{2}, 5, 2, 1, 4 - 2\sqrt{2})$. Quick arithmetic computations show that the only possibility is for $\gamma = 1$. By the lemma, one can always pick new generators A', B' so that $(\alpha, \beta, \gamma) \mapsto (\alpha, \gamma, \beta) \mapsto (\alpha, \gamma, \alpha\gamma - \beta)$. In the case at hand, this means the traces are $(\sqrt{2}, \sqrt{2}, 1) \mapsto (\sqrt{2}, 1, \sqrt{2}) \mapsto (\sqrt{2}, 1, 0)$. This means that $\pi(A')$ has order 4, $\pi(B')$ has order 3 and $\pi(A'B')$ has order 2. This is precisely a presentation⁴ of S_4 and so $S_4 \cong \pi(\langle A', B' \rangle) = \pi(\langle A, B \rangle)$.

Now, consider the case where $\beta = 1$ (this also covers the case where $\beta = -1$ by the lemmas). Then, the Fricke trace identity gives

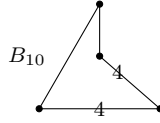
$$\mathrm{tr}([A, B]) = 1 + \gamma^2 - \gamma\sqrt{2} \quad (\text{A.9})$$

⁴For example, this is a solution to exercise 6 in Section 6.3 of [7].

Setting this equal to 1 results in $\gamma(\gamma - \sqrt{2}) = 0$. The two solutions of this are $\gamma = \sqrt{2}$ and $\gamma = 0$. The first case was covered above. In the second case, $(\alpha, \beta, \gamma) = (\sqrt{2}, 1, 0)$, which as above means that $\pi(\langle A, B \rangle) \cong S_4$. \square

Appendix B. $\langle x, y, z \rangle$ is abelian

This section will show that x, y, z as defined in Prop. 30 generate an abelian subgroup of $C^c(M)$, where M is the matrix associated to the the following.



First, recall that $x = g_3g_4g_3g_2$, $y = g_4g_3g_2g_3$ and $z = g_1g_3g_4g_3g_2g_1$, where $\langle g_1, g_2, g_3 \rangle$ and $\langle g_1, g_2, g_4 \rangle$ are isomorphic to dihedral groups and $\langle g_1, g_3, g_4 \rangle \cong \langle g_2, g_3, g_4 \rangle \cong S_4$. The efficient relations for this diagram are recorded in Table B.12. To ease notation, let $g_1 = d, g_2 = b, g_3 = a$ and $g_4 = c$. Now, we are ready to compute the relevant commutators.

Product	Order	Product	Order
g_1g_2	2	$g_3g_2g_4$	3
g_1g_3	3	$g_3g_2g_4g_2$	4
g_1g_4	4	$g_3g_1g_4$	3
g_2g_3	3	$g_3g_1g_4g_1$	4
g_2g_4	4		
g_3g_4	2		

Table B.12: Efficient relations associated to the diagram B_{10} from Prop. 30.

$$\begin{aligned}
xyx^{-1}y^{-1} &= cdc b d c b c b^{-1} c^{-1} d^{-1} c^{-1} c^{-1} b^{-1} c^{-1} d^{-1} \\
&= c d c b d c b c b c d c c b c d \\
&= c d c b d c b c b c d b c d \\
&= c d c b d c c b c b d b c d \\
&= c d c b d b c b d b c d \\
&= c d c d b b c b d b c d \\
&= c d c d c b d b c d \\
&= c d c d c d b b c d \\
&= c d c d c d c d \\
&= 1
\end{aligned}$$

All have order 2
 c has order 2
 bc has order 4 so $bcbc = cbc b$
 c has order 2
 bd has order 2 so $bd = db$
 b has order 2
 bd has order 2 so $bd = db$
 b has order 2
 cd has order 4

Let $O(X)$ denote the order of X . Then,

$$\begin{aligned}
O(xzx^{-1}x^{-1}) &= O(acdcbacdcb \\
&\quad \times a^{-1}b^{-1}c^{-1}d^{-1}c^{-1}a^{-1}b^{-1}c^{-1}d^{-1}c^{-1}) \\
&= O(acdcbacdcbabcdcabcdc) && \text{all have order 2} \\
&= O(cadcbacdcbabcdcabcdc) && O(ac) = 2 \text{ so } ac = ca \\
&= O(adcbacdcbabcdcabcd) && \text{conjugation by } c \\
&= O(dadcbacdcbabcdcabcd) && ad = dada \\
&= O(adacbacdcbabcdcabcd) && \text{conjugation by } d \\
&= O(adbcabdcbbabcdcabcd) && acbac = bcab \\
&= O(adbacdbcabacdcbabc) && b \text{ and } d \text{ commute} \\
&= O(adbacdbcabacdcbabc) && a \text{ and } c \text{ commute} \\
&= O(adbacdbcabacdcbabc) && bcabca = acb \\
&= O(adbacdbcabacdcbabc) && O(abc) = 3 \text{ so } abc = cbacba \\
&= O(dbacdadbdbdbcb) && O(c) = 2 \text{ \& conjugation by } a \\
&= O(dbacdadbdbdbcb) && b \text{ and } d \text{ commute} \\
&= O(bdacdbacdadb) && b \text{ has order 2 and } [b, d] = 1 \\
&= O(dacdadbacdadb) && dacdbacdadb = c \\
&= O(cc) = 1 && \text{since } c \text{ has order 2}
\end{aligned}$$

$$\begin{aligned}
yz y^{-1} z^{-1} &= dcbcacdcba \\
&\times c^{-1} b^{-1} c^{-1} d^{-1} a^{-1} b^{-1} c^{-1} d^{-1} c^{-1} a^{-1} \\
&= dcbcacdcba bcdabedca && \text{all have order 2} \\
&= dcbaccdcba bcdabedca && ac \text{ has order 2, so } ac = ca \\
&= dcbadcbacbcdabedca && c \text{ has order 2} \\
&= dcbadabcabccbcdabedca && abc \text{ has order 3, so } abcabc = cba \\
&= dcbadabcacdbedca && \text{all have order 2} \\
&= dcbadabccadabedca && ac \text{ has order 2, so } ac = ca \\
&= dcbadabadabedca && c \text{ has order 2} \\
&= dcbadabdadbedca && ad \text{ has order 3, so } ada = dad \\
&= dcbadadbabedca && b \text{ and } d \text{ commute} \\
&= dcbdababedca && ad \text{ has order 3, so } adad = da \\
&= dcdbababedca && b \text{ and } d \text{ commute} \\
&= dcdabdbedca && ab \text{ has order 3, so } baba = ab \\
&= dcdadbbedca && b \text{ and } d \text{ commute} \\
&= dcdadcdca && b \text{ has order 2} \\
&= dcdacdcda && cd \text{ has order 4, so } dcdc = cdcd \\
&= dadcacda && adc \text{ has order 3 so } cdacd = adca \\
&= dadaccda && a \text{ and } c \text{ commute} \\
&= dadada && c \text{ has order 2} \\
&= 1 && \text{since } ad \text{ has order 3}
\end{aligned}$$

References

- [1] P. Abramenko and K. Brown, Buildings: Theory and Applications, Graduate Texts in Mathematics (2008).
- [2] P. Cameron and P. Cara, Independent generating sets and geometries for symmetric groups, J. Algebra 258 (2002) 641-650.
- [3] P. Cara, On the unique independent set of four elements in $\text{PSL}(2,31)$, Combinatorics '04 Conference (2004).

- [4] D. Collins and R. K. Dennis, Irredundant Generating Sequences of Finite Groups, Paper in preparation.
- [5] H. Coxeter, Discrete Groups Generated by Reflections, *The Annals of Mathematics* 35 (1934) 588-621.
- [6] L. Dickson, Linear groups: With an exposition of the Galois field theory, Dover Publications Inc. (1958).
- [7] D. Dummit and R. Foote, Abstract algebra, John Wiley & Sons Inc. (2004).
- [8] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12, (2008).
- [9] M. Gradolato and B. Zimmermann, Extending finite group actions on surfaces to hyperbolic 3-manifolds, *Math. Proc. Cambridge Philos. Soc.* 117 (1995) 137-151.
- [10] R. Guralnick, Generation of simple groups, *J. Algebra* 103 (1986) 381-401.
- [11] P. Hall, The Eulerian Functions of a Group, *Quart. J. Math* 7 (1936) 134-151.
- [12] N. Koblitz, A Course in Number Theory and Cryptography, Graduate Texts in Mathematics, Springer-Verlag (1994).
- [13] D. McCullough, Exceptional subgroups of $SL(2, F)$, Unpublished (2005).
- [14] B. Nachman, Generating Sequences of the Two Dimensional Special Projective Linear Group over Fields of Prime Order, $PSL(2, p)$, Senior Thesis, Cornell University Mathematics Department (2012).
- [15] M. Suzuki, Group theory, Springer-Verlag (1982).
- [16] J. Todd and H. Coxeter, A practical method for enumerating cosets of a finite abstract group, *Proceedings of the Edinburgh Mathematical Society* 5 (1936) 26-34.
- [17] J. Whiston, Maximal independent generating sets of the symmetric group, *J. Algebra* 232 (2000) 255-268.

- [18] J. Whiston, The Minimal Generating Sets of Maximal Size of Selected Groups, Ph.D. Thesis, Cambridge University (2001).
- [19] J. Whiston, J. and J. Saxl, On the maximal size of independent generating sets of $\text{PSL}_2(q)$, J. Algebra 258 (2002) 651-657.
- [20] R. Wilson, The Finite Simple Groups, Graduate Texts in Mathematics, Springer (2009).